Symantec™ Storage
Foundation and High
Availability Solutions 6.1.1
Installation Guide - Linux

6.1.1 Maintenance Release
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/contact_techsupp_static.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
Available memory, disk space, and NIC information
Operating system
Version and patch level
Network topology
Router, gateway, and IP address information
Problem description:
  Error messages and log files
  Troubleshooting that was performed before contacting Symantec
  Recent software configuration changes and network changes

Licensing and registration
If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:
www.symantec.com/business/support/

Customer service
Customer service information is available at the following URL:
www.symantec.com/business/support/
Customer Service is available to assist with non-technical questions, such as the following types of issues:
Questions regarding product licensing or serialization
Product registration updates, such as address or name changes
General product information (features, language availability, local dealers)
Latest information about product updates and upgrades
Information about upgrade assurance and support contracts
Information about the Symantec Buying Programs
Advice about Symantec's technical support options
Nontechnical presales questions
Issues that are related to CD-ROMs or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan       customercare_apac@symantec.com
Europe, Middle-East, and Africa semea@symantec.com
North America and Latin America supportsolutions@symantec.com

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec’s enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management

Documentation

Product guides are available on the media in PDF format. Make sure that you are using the current version of the documentation. The document version appears on page 2 of each guide. The latest product documentation is available on the Symantec website.

https://sort.symantec.com/documents

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

# Contents

Technical Support ........................................................................................................... 4

**Chapter 1** About Symantec Storage Foundation and High Availability Solutions .................................................... 10

- About Symantec™ Storage Foundation and High Availability Solutions
  - 6.1.1 .................................................................................................................. 10
- Supported operating systems and database software .................................................. 11

**Chapter 2** Installing the products for the first time ....................................................... 12

- Supported types of Installation .................................................................................. 12
- Installing the Symantec software using the Install Bundles
  - feature ............................................................................................................... 12
- Installing the Symantec software using the script-based installer ......................... 13
- Installing the Symantec software using the Web-based installer ......................... 15
  - Starting the Veritas Web-based installer ......................................................... 15
  - Obtaining a security exception on Mozilla Firefox ........................................... 16
  - Installing 6.1.1 with the Veritas Web-based installer ....................................... 16

**Chapter 3** Upgrading to 6.1.1 from releases earlier than 6.1 ........................................... 18

- Planning to upgrade to SFHA Solutions 6.1.1 ....................................................... 18
- Supported upgrade types ....................................................................................... 18
- Supported upgrade paths for SFHA Solutions 6.1.1 from releases earlier than 6.1 .................................................. 19
  - About using the installer to upgrade from releases earlier than 6.1
    - when the root disk is encapsulated ......................................................... 22
- Preparing to upgrade Volume Replicator .............................................................. 22
- Downloading SFHA Solutions 6.1.1 .................................................................... 24
- Performing a full upgrade with Install Bundles .................................................... 25
  - Performing a full upgrade of VCS using Install Bundles ................................. 25
  - Performing a full upgrade of SFHA using Install Bundles ............................. 26
  - Performing a full upgrade of SFCFSHA using Install Bundles .................... 29
  - Performing a full upgrade of SF Oracle RAC using Install Bundles .................. 32
Performing a phased upgrade using Install Bundles .................................. 39
Performing a phased VCS upgrade using Install Bundles .................. 39
Performing a phased SFHA upgrade using Install Bundles ............. 53
Performing a phased SFCFSHA upgrade using Install Bundles .......... 68
Performing a phased upgrade of SF Oracle RAC using Install Bundles ..................................................... 75
Performing an automated upgrade using response files with Install Bundles .................................................... 86
Performing an automated upgrade of VCS, SFHA, or SFCFSHA using response files ........................................... 86
Upgrading SF Oracle RAC using a response file ............................. 87
Performing rolling upgrade of SFHA Solutions using response files ........................................................................... 88
Performing a rolling upgrade using Install Bundles ............................ 88
Supported rolling upgrade paths ..................................................... 89
Performing a rolling upgrade of VCS, SFHA, and SFCFSHA with Install Bundles ................................................................. 90
Performing a rolling upgrade of SF Oracle RAC with Install Bundles .................................................................................... 92

Chapter 4 Upgrading to 6.1.1 from 6.1 .................................................... 100

About using the installer to upgrade from 6.1 when the root disk is encapsulated ................................................................. 100
Prerequisites for upgrading to 6.1.1 .................................................. 101
Downloading required software to upgrade to 6.1.1 .......................... 101
Performing a full upgrade to 6.1.1 on a cluster .................................. 101
Performing a full upgrade to 6.1.1 on a Symantec Cluster Server ................................................................. 102
Performing a full upgrade to 6.1.1 on an SFHA cluster ................. 102
Performing a full upgrade to 6.1.1 on an SFCFSHA cluster .......... 103
Performing a full upgrade to 6.1.1 on an SF Oracle RAC cluster ................................................................. 105
Upgrading to 6.1.1 on a standalone system ....................................... 109
Performing a phased upgrade to SFCFSHA and SFRAC .............. 111
Performing a phased upgrade of SFCFSHA .................................. 111
Performing phased upgrade of SF Oracle RAC to version 6.1.1 ................. 121
Upgrading to 6.1.1 on a system that has encapsulated boot disk ....... 134
Performing a rolling upgrade using the installer ............................. 134
About rolling upgrades ................................................................. 135
Prerequisites for a rolling upgrade .................................................. 135
Performing a rolling upgrade using the installer ........................................ 136
Upgrading the operating system ........................................................... 145
Upgrading SFHA with the Veritas Web-based installer ....................... 145
Verifying software versions .............................................................. 146

Chapter 5 Removing Symantec Storage Foundation and High
Availability Solutions ........................................................................... 147

About removing Symantec Storage Foundation and High Availability
Solutions 6.1.1 ..................................................................................... 147
Uninstalling Symantec Storage Foundation Cluster File System High
Availability 6.1.1 .............................................................................. 148
Preparing to uninstall Symantec Storage Foundation Cluster File
System High Availability ................................................................... 148
Uninstalling Symantec Storage Foundation Cluster File System
High Availability .............................................................................. 150
Uninstalling Symantec Storage Foundation for Oracle RAC ............... 151

Appendix A About the installation script .............................................. 153

About the installation script ................................................................. 153
The installmr script options ............................................................... 153
About Symantec Storage Foundation and High Availability Solutions

This chapter includes the following topics:

- About Symantec™ Storage Foundation and High Availability Solutions 6.1.1
- Supported operating systems and database software

About Symantec™ Storage Foundation and High Availability Solutions 6.1.1

Symantec™ Storage Foundation and High Availability Solutions 6.1.1 provides patch updates for the following products:

- Symantec Dynamic Multi-Pathing (DMP)
- Veritas Volume Manager (VxVM)
- Veritas File System (VxFS)
- Symantec Storage Foundation (SF)
- Symantec Cluster Server (VCS)
- Symantec Storage Foundation and High Availability (SFHA)
- Symantec Storage Foundation Cluster File System and High Availability (SFCFSHA)
- Symantec Storage Foundation for Oracle RAC (SF Oracle RAC)
- Symantec ApplicationHA (ApplicationHA)
You can install or upgrade to the patches included in this release by using the `installmr` script. For information on the various options that you can use with the script:

The release supports the following installation and upgrade scenarios:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Install and upgrade process</th>
</tr>
</thead>
<tbody>
<tr>
<td>No product is installed on the target system</td>
<td>Run <code>installmr -base_path</code> option to install 6.1.1</td>
</tr>
<tr>
<td>The product version before 6.1 is installed on the target system</td>
<td>Run <code>installmr -base_path</code> option to upgrade to 6.1.1</td>
</tr>
<tr>
<td>The product version 6.1 is installed on the target system</td>
<td>Run <code>installmr</code> to upgrade to 6.1.1</td>
</tr>
</tbody>
</table>

To install or upgrade the product to 6.1.1 from releases before 6.1, invoke the `installmr` script with `-base_path` option to install or upgrade 6.1.1.

For installation:

```
./installmr -base_path /tmp/sfha6.1/
```

For upgrade:

```
./installmr -base_path /tmp/sfha6.1/ -upgrade
```

For more information regarding installing 6.1.1 using Install Bundles feature:

See *Using Install Bundles to simultaneously install or upgrade base releases, maintenance patches, and hot fixes* in 6.1 Installation Guides.

Symantec strongly recommends you to use the Install Bundles feature to install or upgrade Symantec Storage Foundation and High Availability Solutions 6.1.1.

## Supported operating systems and database software

For information on supported operating systems and database software, see the *Symantec™ Storage Foundation and High Availability Solutions 6.1.1 Release Notes - Linux*. 
Installing the products for the first time

This chapter includes the following topics:

- Supported types of Installation
- Installing the Symantec software using the Install Bundles feature
- Installing the Symantec software using the script-based installer
- Installing the Symantec software using the Web-based installer

Supported types of Installation

SFHA Solutions 6.1.1 supports the following types of Installation:

- Installing Symantec products with the script-based installer

Note: Symantec recommends you to install 6.1.1 with Install Bundles.

- Installing Symantec products with the web-based installer.

Installing the Symantec software using the Install Bundles feature

This section describes how to install a Symantec Storage Foundation and High Availability Solutions product using the Install Bundles feature in one step.
To install the Symantec software 6.1.1 using Install Bundles:

2. Extract the tar ball into the /tmp/sfha6.1/ directory.
4. Extract it to the /tmp/sfha6.1.1 directory.
5. Change to the /tmp/sfha6.1.1 directory by entering:
   ```
   # cd /tmp/sfha6.1.1
   ```
6. Invoke the `installmr` script with `-base_path` option to install 6.1 and 6.1.1. Enter:
   ```
   ./installmr -base_path /tmp/sfha6.1/
   ```
7. In the Task Menu, enter i to install a product.

See the 6.1 Installation Guide for configuration steps.

### Installing the Symantec software using the script-based installer

This section describes how to install a 6.1.1 Symantec Storage Foundation and High Availability Solutions product for the first time on a host. Download the latest patches for the installer before you install or upgrade the product.

See "Installing the Symantec software for the first time" on page 14.
See the 6.1 Installation Guide and Release Notes for your product for more information.

Installing the Symantec software for the first time


2. Extract the tar ball into a directory called /tmp/sfha6.1.

3. Check https://sort.symantec.com/patches to see if there are any patches available for the 6.1 Installer. Download applicable P-patches and extract them to the /tmp directory.

4. Change to the /tmp/sfha6.1 directory:

   # cd /tmp/sfha6.1

5. Run the installer to install SFHA Solutions 6.1.

   See the Installation Guide for instructions on installing the 6.1 version of this product.

   #./installer -require complete_path_to_61_installer_patch

   Note: If the P-patch is not available for 6.1 installer, use the installer script without -require option.


7. Extract it to a directory called /tmp/sfha6.1.1.

8. Check https://sort.symantec.com/patches to see if there are patches available for the 6.1.1 installer. Download applicable P-patches and extract them to the /tmp directory.

9. Change to the /tmp/sfha6.1.1 directory:

   # cd /tmp/sfha6.1.1

10. Invoke the installmr script to install 6.1.1:

    # ./installmr -require complete_path_to_611_installer_patch

    Note: If the P-patch is not available for 6.1.1 installer, use the installmr script without -require option.
If you did not configure the product after the 6.1 installation, the installer prompts you to configure the product during MR installation. If you do not want to configure the product now, answer n when prompted. To configure the product in the future, run the product installation script from `/opt/VRTS/install` directory with the --configure option.

For configuration procedures, refer to 6.1 Installation Guide for your product.

Installing the Symantec software using the Web-based installer

This section describes how to install a Symantec Storage Foundation and High Availability Solutions product for the first time on a host and then to install 6.1.1 using the Web-based installer. For detailed instructions on how to install 6.1 using the Web-based installer, follow the procedures in the 6.1 Installation Guide and Release Notes for your products.

See Upgrading to 6.1.1 from 6.1 for upgrade procedures.

You need to configure SF Oracle RAC before you upgrade it from 6.1 to 6.1.1. For more information, refer to Software Limitations in 6.1.1 Release Notes.

Starting the Veritas Web-based installer

This section describes starting the Veritas Web-based installer.

To start the Web-based installer

1. Start the Veritas XPortal Server process `xprt1wid`, on the installation server:
   
   ```
   # ./webinstaller start
   ```

   The webinstaller script displays a URL.

2. Start the Web browser on the system from which you want to perform the installation.

3. Navigate to the URL displayed from step 1.

4. The browser may display the following message:

   Secure Connection Failed

   Obtain a security exception for your browser.

5. When prompted, enter root and root's password of the installation server.
Obtaining a security exception on Mozilla Firefox

You may need to get a security exception on Mozilla Firefox.

To obtain a security exception

1. Click **Or you can add an exception** link.
2. Click **Add Exception** button.
3. Click **Get Certificate** button.
4. Uncheck **Permanently Store this exception checkbox (recommended)**.
5. Click **Confirm Security Exception** button.
6. Enter root in **User Name** field and root password of the web server in the **Password** field.

Installing 6.1.1 with the Veritas Web-based installer

This section describes installing SFHA with the Veritas Web-based installer.

To install SFHA

1. The 6.1 version of the Symantec product must be installed before upgrading to 6.1.1.

2. On the **Select a task and a product** page, select **Install 6.1.1** from the **Task** drop-down list, and click **Next**.

3. Indicate the systems on which to install. Enter one or more system names, separated by spaces. Click **Next**.

4. You have the option to let the installer configure SSH or RSH communications between the systems. If you choose to allow this configuration, select the communication type and provide the root passwords for each system.

5. After the validation completes successfully, click **Next** to install 6.1.1 patches on the selected system.
6 For Storage Foundation, click **Next** to complete the patch installation.

For Storage Foundation High Availability, if the product is not yet configured, the installer prompts you to configure the cluster.

If you select **n**, you can exit the installer. You must configure the product before you can use Storage Foundation High Availability.

For configuration procedures, refer to 6.1 *Installation Guide* for your product.

After the installation completes, the installer displays the location of the log and summary files. If required, view the files to confirm the installation status.

7 Select the checkbox to specify whether you want to send your installation information to Symantec.

Would you like to send the information about this installation to Symantec to help improve installation in the future?

Click **Finish**.
Upgrading to 6.1.1 from releases earlier than 6.1

This chapter includes the following topics:

- Planning to upgrade to SFHA Solutions 6.1.1
- Performing a full upgrade with Install Bundles
- Performing a phased upgrade using Install Bundles
- Performing an automated upgrade using response files with Install Bundles
- Performing a rolling upgrade using Install Bundles

Planning to upgrade to SFHA Solutions 6.1.1

This section includes the following topics:

- Supported upgrade paths for SFHA Solutions 6.1.1 from releases earlier than 6.1
- About using the installer to upgrade from releases earlier than 6.1 when the root disk is encapsulated
- Preparing to upgrade Volume Replicator
- Downloading SFHA Solutions 6.1.1

Supported upgrade types

SFHA Solutions supports various ways of upgrading your cluster to the latest version. Choose a method that best suits your environment and supports your planned upgrade path.
Table 3-1 lists the supported types of upgrade.

Table 3-1  

<table>
<thead>
<tr>
<th>Type of upgrade</th>
<th>Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full upgrade</td>
<td>A full upgrade involves upgrading all the nodes in the cluster at the same time. All components are upgraded during the process. The cluster remains unavailable for the duration of the upgrade.</td>
</tr>
<tr>
<td>Phased upgrade</td>
<td>The phased upgrade methodology involves upgrading half of the nodes in the cluster at a time.</td>
</tr>
<tr>
<td>Rolling upgrade</td>
<td>The rolling upgrade minimizes downtime for highly available clusters to the amount of time that it takes to perform a service group failover.</td>
</tr>
<tr>
<td>Automated upgrade using response files</td>
<td>You can upgrade from SFHA Solutions using a response file.</td>
</tr>
</tbody>
</table>

Supported upgrade paths for SFHA Solutions 6.1.1 from releases earlier than 6.1

You can run the `installmr` script with Install Bundles to upgrade SFHA Solutions to 6.1.1 from releases earlier than 6.1.

For information on operating systems that are supported for 6.1.1, see System requirements in Symantec™ Storage Foundation and High Availability Solutions 6.1.1 Release Notes.

The following tables describe upgrading to 6.1.

Table 3-2  

<table>
<thead>
<tr>
<th>Symantec product versions</th>
<th>RHEL 5</th>
<th>RHEL 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 RPs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 PR1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 SP1</td>
<td>Upgrade OS to RHEL 5 U5 or above.</td>
<td></td>
</tr>
<tr>
<td>5.1 SP1 RP1</td>
<td>Upgrade to 6.1.1 using the <code>installmr</code> script with Install Bundles.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>
Table 3-2  RHEL 5 x64 and RHEL 6 x64 upgrades from releases earlier than 6.1 (continued)

<table>
<thead>
<tr>
<th>Symantec product versions</th>
<th>RHEL 5</th>
<th>RHEL 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 SP1 PR2</td>
<td>Not applicable.</td>
<td>Upgrade OS to RHEL 6 U3 or above. Upgrade the product to 6.1.1 using the installmr script with Install Bundles.</td>
</tr>
<tr>
<td>5.1 SP1 PR3</td>
<td>Upgrade OS to RHEL 5 U5 or above.</td>
<td>Upgrade OS to RHEL 6 U3 or above. Upgrade the product to 6.1.1 using the installmr script with Install Bundles.</td>
</tr>
<tr>
<td>5.1 SP1 RP2</td>
<td>Upgrade to 6.1.1 using the installmr script with Install Bundles.</td>
<td></td>
</tr>
<tr>
<td>5.1 SP1 RP3</td>
<td>Upgrade OS to RHEL 6 U3 or above. Upgrade the product to 6.1.1 using the installmr script with Install Bundles.</td>
<td></td>
</tr>
<tr>
<td>5.1 SP1 RP4</td>
<td>Upgrade directly to 6.1.1 using the installmr script with Install Bundles.</td>
<td>Upgrade OS to RHEL 6 U3 or above. Upgrade to 6.1.1 using the installmr script with Install Bundles.</td>
</tr>
<tr>
<td>6.0</td>
<td>Upgrade OS to OL 5 U5 or above.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>6.0 RP1</td>
<td>Upgrade to 6.1.1 using the installmr script with Install Bundles.</td>
<td></td>
</tr>
<tr>
<td>6.0.1</td>
<td>Upgrade OS to OL 6 U3 or above.</td>
<td></td>
</tr>
<tr>
<td>6.0.2</td>
<td>Upgrade to 6.1.1 using the installmr script with Install Bundles.</td>
<td></td>
</tr>
<tr>
<td>6.0.3</td>
<td>Upgrade OS to OL 6 U3 or above.</td>
<td></td>
</tr>
<tr>
<td>6.0.5</td>
<td>Upgrade to 6.1.1 using the installmr script with Install Bundles.</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-3  OL 5 x64 and OL 6 x64 upgrades from releases earlier than 6.1

<table>
<thead>
<tr>
<th>Symantec product versions</th>
<th>OL 5 (RHEL Compatible mode)</th>
<th>OL 6 (RHEL Compatible mode)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Upgrade OS to OL 5 U5 or above.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>5.1 RPs</td>
<td>Upgrade to 6.1.1 using the installmr script with Install Bundles.</td>
<td></td>
</tr>
<tr>
<td>5.1 PR1</td>
<td>Upgrade OS to OL 6 U3 or above.</td>
<td></td>
</tr>
<tr>
<td>5.1 SP1</td>
<td>Upgrade the product to 6.1.1 using the installmr script with Install Bundles.</td>
<td></td>
</tr>
<tr>
<td>5.1 SP1 RP1</td>
<td>Upgrade OS to OL 6 U3 or above. Upgrade the product to 6.1.1 using the installmr script with Install Bundles.</td>
<td></td>
</tr>
<tr>
<td>5.1 SP1 PR2</td>
<td>Not applicable.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3-3  
OL 5 x64 and OL 6 x64 upgrades from releases earlier than 6.1 (continued)

<table>
<thead>
<tr>
<th>Symantec product versions</th>
<th>OL 5 (RHEL Compatible mode)</th>
<th>OL 6 (RHEL Compatible mode)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 SP1 PR3</td>
<td>Upgrade OS to OL 5 U5 or above.</td>
<td>Upgrade OS to OL 6 U3 or above.</td>
</tr>
<tr>
<td>5.1 SP1 RP2</td>
<td>Upgrade to 6.1.1 using the <em>installmr</em> script with Install Bundles.</td>
<td>Upgrade the product to 6.1.1 using the <em>installmr</em> script with Install Bundles.</td>
</tr>
<tr>
<td>5.1 SP1 RP3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 SP1 RP4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.0</td>
<td>Upgrade directly to 6.1.1 using the <em>installmr</em> script with Install Bundles.</td>
<td>Upgrade OS to RHEL6 U3 or above.</td>
</tr>
<tr>
<td>6.0 RP1</td>
<td></td>
<td>Upgrade to 6.1.1 using the <em>installmr</em> script with Install Bundles.</td>
</tr>
<tr>
<td>6.0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.0.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.0.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.0.5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 3-4  
SLES 11 x64 upgrades from releases earlier than 6.1

<table>
<thead>
<tr>
<th>Symantec product versions</th>
<th>SLES 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Upgrade OS to SLES11 SP2 or above. Use the <em>installmr</em> script with Install Bundles to upgrade the product to 6.1.1.</td>
</tr>
<tr>
<td>5.1 RPs</td>
<td></td>
</tr>
<tr>
<td>5.1 SP1</td>
<td></td>
</tr>
<tr>
<td>5.1 SP1 RPs</td>
<td></td>
</tr>
<tr>
<td>6.0</td>
<td>Upgrade OS to SLES11 SP2 or above. Use the <em>installmr</em> script with Install Bundles to upgrade the product to 6.1.1.</td>
</tr>
<tr>
<td>6.0 RP1</td>
<td></td>
</tr>
<tr>
<td>6.0.1</td>
<td></td>
</tr>
<tr>
<td>6.0.2</td>
<td></td>
</tr>
<tr>
<td>6.0.3</td>
<td></td>
</tr>
<tr>
<td>6.0.5</td>
<td></td>
</tr>
<tr>
<td>6.0.4</td>
<td>Use the <em>installmr</em> script with Install Bundles to upgrade the product to 6.1.1.</td>
</tr>
</tbody>
</table>
About using the installer to upgrade from releases earlier than 6.1 when the root disk is encapsulated

When you use the installer to upgrade from a previous version of SFHA Solutions and the system where you plan to upgrade has an encapsulated root disk, you may have to unencapsulate it.

Table 3-5 Upgrading using the installer from releases earlier than 6.1 when the root disk is encapsulated

<table>
<thead>
<tr>
<th>Starting version</th>
<th>Ending version</th>
<th>Action required</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>6.1.1</td>
<td>Do not unencapsulate. The installer runs normally. Reboot after upgrade.</td>
</tr>
<tr>
<td>5.1 RP1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 RP2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 PR1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 SP1</td>
<td>6.1.1</td>
<td>Do not unencapsulate. The installer runs normally. Reboot after upgrade.</td>
</tr>
<tr>
<td>5.1 SP1 RP1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 SP1 RP2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 SP1 RP3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 SP1 RP4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 SP1 PR2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 SP1 PR3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.0</td>
<td>6.1.1</td>
<td>Do not unencapsulate. The installer runs normally. Reboot after upgrade.</td>
</tr>
<tr>
<td>6.0 RP1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.0.1</td>
<td>6.1.1</td>
<td>Do not unencapsulate. The installer runs normally. Reboot after upgrade.</td>
</tr>
<tr>
<td>6.0.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.0.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.0.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.0.5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Preparing to upgrade Volume Replicator

Before installing or upgrading Volume Replicator (VVR):

- Confirm that your system has enough free disk space to install VVR.
- Make sure you have root permissions. You must have root permissions to perform the install and upgrade procedures.

- If replication using VVR is configured, Symantec recommends that the disk group version is at least 110 prior to upgrading.
  You can check the Disk Group version using the following command:

  ```
  # vxdg list diskgroup
  ```

- If replication using VVR is configured, make sure the size of the SRL volume is greater than 110 MB.
  Refer to the Symantec™ Storage Foundation and High Availability Solutions Replication Administrator’s Guide.

- If replication using VVR is configured, verify that all the Primary RLINKs are up-to-date on all the hosts.

  ```
  # /usr/sbin/vxrlink -g diskgroup status rlink_name
  ```

  **Note:** Do not continue until the primary RLINKs are up-to-date.

- If VCS is used to manage VVR replication, follow the preparation steps to upgrade VVR and VCS agents.

  See the Symantec™ Storage Foundation and High Availability Solutions Replication Administrator’s Guide for more information.

  See the Getting Started Guide for more information on the documentation.

### Planning an upgrade from the previous VVR version

If you plan to upgrade VVR from the previous VVR version, you can upgrade VVR with reduced application downtime by upgrading the hosts at separate times. While the Primary is being upgraded, the application can be migrated to the Secondary, thus reducing downtime. The replication between the (upgraded) Primary and the Secondary, which have different versions of VVR, will still continue. This feature facilitates high availability even when the VVR upgrade is not complete on both the sites. Symantec recommends that the Secondary hosts be upgraded before the Primary host in the Replicated Data Set (RDS).

See the Symantec™ Storage Foundation Release Notes for information regarding VVR support for replicating across Storage Foundation versions.

Replicating between versions is intended to remove the restriction of upgrading the Primary and Secondary at the same time. VVR can continue to replicate an existing RDS with Replicated Volume Groups (RVGs) on the systems that you want to
upgrade. When the Primary and Secondary are at different versions, VVR does not support changing the configuration with the `vradmin` command or creating a new RDS.

Also, if you specify TCP as the network protocol, the VVR versions on the Primary and Secondary determine whether the checksum is calculated. As shown in Table 3-6, if either the Primary or Secondary are running a version of VVR prior to 6.1.1, and you use the TCP protocol, VVR calculates the checksum for every data packet it replicates. If the Primary and Secondary are at VVR 6.1.1, VVR does not calculate the checksum. Instead, it relies on the TCP checksum mechanism.

### Table 3-6  VVR versions and checksum calculations

<table>
<thead>
<tr>
<th>VVR prior to 6.1.1 (DG version &lt;= 140)</th>
<th>VVR 6.1.1 (DG version &gt;= 150)</th>
<th>VVR calculates checksum TCP connections?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Secondary &gt;= 150</td>
<td>Yes</td>
</tr>
<tr>
<td>Secondary</td>
<td>Primary</td>
<td>Yes</td>
</tr>
<tr>
<td>Primary and Secondary</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Primary and Secondary</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note:** When replicating between versions of VVR, avoid using commands associated with new features. The earlier version may not support new features and problems could occur.

If you do not need to upgrade all the hosts in the RDS simultaneously, you can use replication between versions after you upgrade one host. You can then upgrade the other hosts in the RDS later at your convenience.

**Note:** If you have a cluster setup, you must upgrade all the nodes in the cluster at the same time.

### Downloading SFHA Solutions 6.1.1

The following procedure describes how to upgrade to 6.1.1 with Install Bundles from releases earlier than 6.1.

**Note:** If you are upgrading from releases earlier than 6.1, Symantec suggests you upgrade with Install Bundles.
2. Extract the tar ball into a directory called /tmp/sfha6.1.
4. Extract it to a directory called /tmp/sfha6.1.1

Performing a full upgrade with Install Bundles

- Performing a full upgrade of VCS using Install Bundles
- Performing a full upgrade of SFHA using Install Bundles
- Performing a full upgrade of SFCFSHA using Install Bundles
- Performing a full upgrade of SF Oracle RAC using Install Bundles

Performing a full upgrade of VCS using Install Bundles

You can use the installer to upgrade VCS.

To upgrade VCS using the product installer

1. Log in as superuser.
2. Change to the /tmp/sfha6.1.1 directory.
3. Invoke the installmr script with -base_path option to upgrade to 6.1.1:

   ```
   # .installmr -base_path /tmp/sfha6.1/
   ```

4. From the opening Selection Menu, choose: G for "Upgrade a Product."
5. Choose 1 for Full Upgrade.
6. Enter the names of the nodes that you want to upgrade. Use spaces to separate node names. Press the Enter key to proceed.
   
   The installer runs some verification checks on the nodes.

7. When the verification checks are complete, the installer asks if you agree with the terms of the End User License Agreement. Press y to agree and continue.
   
   The installer lists the RPMs to upgrade.
The installer asks if you want to stop VCS processes. Press the Enter key to continue.

The installer stops VCS processes, uninstalls RPMs, installs or upgrades RPMs, configures, and starts VCS.

The installer lists the nodes that Symantec recommends you to restart, if needed.

The installer asks if you would like to send the information about this installation to Symantec to help improve installation in the future. Enter your response.

The installer displays the location of log files, summary file, and response file.

If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

Performing a full upgrade of SFHA using Install Bundles

This section describes how to perform a full upgrade of SFHA using Install Bundles.

- Upgrading SFHA using with Install Bundles

Upgrading SFHA using with Install Bundles

Use this procedure to upgrade SFHA with Install Bundles.

Note: The installer doesn't support upgrading with Install Bundles when the boot disk is encapsulated. If the boot disk is encapsulated, you need to un-encapsulate the boot disk first, and then run Install Bundles to perform upgrade.
To upgrade SFHA from previous versions to 6.1.1

1. Log in as superuser.

2. Use the following command to check if any VxFS file systems or Storage Checkpoints are mounted:

   ```
   # df -T | grep vxfs
   ```

3. Unmount all Storage Checkpoints and file systems:

   ```
   # umount /checkpoint_name
   # umount /filesystem
   ```

4. Verify that all file systems have been cleanly unmounted:

   ```
   # echo "8192B.p S" | fsdb -t vxfs filesystem | grep clean
   ```

   **clean_value** value of 0x5a indicates the file system is clean, 0x3c indicates the file system is dirty, and 0x69 indicates the file system is dusty. A dusty file system has pending extended operations.

   Perform the following steps in the order listed:

   ■ If a file system is not clean, enter the following commands for that file system:

     ```
     # fsck -t vxfs raw_device
     # mount -t vxfs block_device mountpoint
     # umount /mountpoint
     ```

     This should complete any extended operations that were outstanding on the file system and unmount the file system cleanly.

     There may be a pending large RPM clone removal extended operation if the `umount` command fails with the following error:

     ```
     file system device busy
     ```

     You know for certain that an extended operation is pending if the following message is generated on the console:

     ```
     Storage Checkpoint asynchronous operation on file_system file system still in progress.
     ```

   ■ If an extended operation is pending, you must leave the file system mounted for a longer time to allow the operation to complete. Removing a very large RPM clone can take several hours.
Repeat this step to verify that the unclean file system is now clean.

5 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.

6 Stop all the volumes by entering the following command for each disk group:

# vxvol -g diskgroup stopall

To verify that no volumes remain open, use the following command:

# vxprint -Aht -e v_open

7 Make a record of the mount points for VxFS file systems and VxVM volumes that are defined in the /etc/fstab file. You will need to recreate these entries in the /etc/fstab file on the freshly installed system.

8 Perform any necessary preinstallation checks.

9 To invoke the installer, run the installmr command as shown in this example:

# cd /tmp/sfha6.1.1
# ./installmr -base_path /tmp/sfha6.1/

10 Enter G to upgrade and press Return.

11 You are prompted to enter the system names (in the following example, "host1") on which the software is to be installed. Enter the system name or names and then press Return.

Enter the 64 bit <platform> system names separated by spaces : [q, ?] host1 host2

where <platform> is the platform on which the system runs, such as RHEL5. Depending on your existing configuration, various messages and prompts may appear. Answer the prompts appropriately.

During the system verification phase, the installer checks if the boot disk is encapsulated and the upgrade's path. If the upgrade is not supported, you need to un-encapsulate the boot disk.

12 The installer asks if you agree with the terms of the End User License Agreement. Press y to agree and continue.
13 The installer lists the RPMs to upgrade. Then the installer asks if you want to stop SFHA processes, enter y to continue.

Do you want to stop SFHA processes now? [y,n,q] (y) y

If you select y, the installer stops the product processes and makes some configuration updates before upgrading.

14 The installer stops, uninstalls, reinstalls, and starts specified RPMs.

15 If necessary, reinstate any missing mount points in the /etc/fstab file on each node that you recorded in step 7.

16 Restart all the volumes by entering the following command for each disk group:

   # vxvol -g diskgroup startall

17 Remount all VxFS file systems and Storage Checkpoints on all nodes:

   # mount /filesystem
   # mount /checkpoint_name

18 You can perform the following optional configuration steps:

   ■ If you want to use features of Symantec Storage Foundation 6.1.1 for which you do not currently have an appropriate license installed, obtain the license and run the vxlicinst command to add it to your system.

   ■ To upgrade VxFS Disk Layout versions and VxVM Disk Group versions, follow the upgrade instructions.

19 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

   For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

Performing a full upgrade of SFCFSHA using Install Bundles

This section describes how to perform a full upgrade of SFCFSHA using Install Bundles.
Performing a full SFCFSHA upgrade with Install Bundles

Performing a full SFCFSHA upgrade with Install Bundles

Performing a full upgrade involves the following tasks:

- Ensuring that the file systems are clean
- Performing the upgrade

Ensuring the file systems are clean

Before upgrading to SFCFSHA 6.1.1, ensure that the file systems are clean. To ensure that the logs have been replayed and the file systems are marked clean:

To ensure the file systems are clean

1. Log in as superuser onto any node in the cluster.
2. Take the service group offline on each node of the cluster, which contains VxFS and CFS resources:

   ```bash
   # hagrp -offline group -any
   ```

   where `group` is the VCS service group that has the CVMVolDg and CFSMount resource.

   Repeat this step for each SFCFSHA service group.

   **Note:** This unmounts the CFS file systems.

3. Unmount all VxFS file systems not under VCS control:

   ```bash
   # umount /mount_point
   ```

4. Check and repair each VxFS file system:

   ```bash
   # fsck -t vxfs /dev/vx/dsk/diskgroup/volume
   ```

   The `fsck` command in `/opt/VRTS/bin` accepts either the block or character device (`/dev/vx/dsk/dg/vol`) or (`/dev/vx/rdsk/dg/vol`). The operating system version of `fsck` may limit the device types it accepts.

   For more information, see the `fsck` and `fsck_vxfs` man pages.

   Repeat this step for each file system.
Performing the upgrade

To perform the upgrade

1 Log in as superuser.

2 Change to the /tmp/sfha6.1.1 directory:

   # cd /tmp/sfha6.1.1

3 Verify there are no VxFS file systems mounted on the nodes being upgraded:

   # mount -t vxfs

   If any VxFS file systems are mounted, offline the group on each node of the cluster. For details, see step 2 and step 3 of Ensuring the file systems are clean.

4 Change to the /tmp/sfha6.1.1 directory. Invoke the installmr script with -base_path option to upgrade to 6.1.1:

   # ./installmr -base_path /tmp/sfha6.1/

5 From the opening Selection Menu, choose: G for Upgrade a Product. Choose 1 for Full Upgrade.

6 You are prompted to enter the system names (in the following example, "node01" and "node02") on which the software is to be upgraded. Enter the system name or names and then press Return.

   Enter the system names separated by spaces on which to install SFCFSHA: node01 node02

7 At the prompt, specify whether you accept the terms of the End User License Agreement (EULA). Press y to agree and continue.

8 During the initial system check, the installer verifies that communication between systems has been set up.

   If the installer hangs or asks for a login password, sertup passwordless ssh or setup rsh from the system that run installmr to the system that need to be upgraded to 6.1.1. Then run the installer again.

9 After you accept EULA and the system checks complete, the installer displays a list of the RPMs that will be upgraded. Press Enter to continue with the upgrade.

10 Output shows information that SFCFSHA must be stopped on a running system. Enter y to continue.
11 The installer stops, uninstalls, reinstalls, and starts specified RPMs.

12 Press **Enter** again for summary information about logs and reboots.

Do not remove the log files until the Symantec products are working properly on your system. Technical Support will need these log files for debugging purposes.

13 Update the configuration.

14 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

### Performing a full upgrade of SF Oracle RAC using Install Bundles

This section describes how to perform a full upgrade of SF Oracle RAC using Install Bundles.

- Preparing to perform a full upgrade to 6.1.1 on an SF Oracle RAC cluster
- Upgrading SF Oracle RAC and operating system (minor OS upgrade)

### Preparing to perform a full upgrade to 6.1.1 on an SF Oracle RAC cluster

Perform the preparatory steps in this section if you are performing a full upgrade of the cluster. Before you upgrade, make sure that your systems meet the hardware and software requirements for this release.
To prepare to upgrade SF Oracle RAC

1. Log in as superuser to one of the nodes in the cluster.

2. Back up the following configuration files on your system: main.cf, types.cf, CVMTypes.cf, CFSTypes.cf, OracleTypes.cf, OracleASMTypes.cf, PrivNIC.cf, MultiPrivNIC.cf, CRSResource.cf, /etc/llttab, /etc/llthosts, /etc/gabtab, /etc/vxfentab, /etc/vxfendg, /etc/vxfenmode

For example:

```bash
# cp /etc/VRTSvcs/conf/config/main.cf \
/etc/VRTSvcs/conf/config/main.cf.save
```

3. Installer verifies that recent backups of configuration files in VxVM private region have been saved in /etc/vx/cbr/bk.

If not, a warning message will be displayed after `installmr upgrade` prechecks.

**Warning:** Backup `/etc/vx/cbr/bk` directory.

4. Stop all applications that use VxFS or VxVM disk groups, whether local or CFS.

   If the applications are under VCS control:

   ```bash
   # hagrp -offline grp_name -any
   ```

   If the applications are not under VCS control:

   Use native application commands to stop the application.

5. Stop all Oracle RAC resources.

   - If the database instances are managed by VCS, take the corresponding VCS service groups offline. As superuser, enter:

     ```bash
     # hagrp -offline oracle_group -any
     ```

   - If the database instances are not managed by VCS, then run the following on one node:

     For Oracle RAC 11g:

     ```bash
     $ srvctl stop database -d db_name
     ```

     For Oracle RAC 12c:
$ srvctl stop database -db db_name

6  ■ If the Oracle database is managed by VCS, set the AutoStart value to 0 to prevent the database service group from starting automatically when VCS starts:

   # haconf -makerw
   # hagrp -modify oracle_group AutoStart 0
   # haconf -dump -makero

■ If the Oracle database is not managed by VCS, change the management policy for the database to MANUAL:

■ For Oracle RAC 11g:

   $ srvctl modify database -d db_name -y MANUAL

■ For Oracle RAC 12c:

   $ srvctl modify database -db db_name -policy MANUAL

7  Stop VCS on all nodes:

   # hastop -all

8  Unmount the VxFS file system, which is not under VCS control.

   # mount |grep vxfs
   # fuser -m /mount_point
   # umount /mount_point

Make sure that no processes are running which make use of mounted shared file system or shared volumes.

   # fuser -cu /mount_point
If you plan to continue using the Storage Foundation for Databases (SFDB) tools, you must prepare to migrate the SFDB repository database before upgrading to 6.1.1.

See "Pre-upgrade tasks for migrating the SFDB repository database" on page 35.

If you plan to upgrade the operating system, stop all ports.

If you are running version 5.1 and later, stop the ports using the installer:

```
# /opt/VRTS/install/installsfarc -stop
```

Pre-upgrade tasks for migrating the SFDB repository database

If you plan to continue using Database Storage Checkpoints or SmartTier for Oracle policies you created with a 5.0x or earlier version of Storage Foundation for Oracle RAC, you must migrate the SFDB repository database to 6.1.1.

Note: The Sfua_Base repository resource group will be removed from the main.cf file. It is not required as a separate service group for SF Oracle RAC 6.1.1.

Perform the following before upgrading SF Oracle RAC.

To prepare to migrate the repository database

- Resynchronize all existing snapshots before upgrading. As Oracle user, enter:

```
$ /opt/VRTS/bin/dbed_vmsnap -S $ORACLE_SID \
-f SNAPPLAN -o resync
```

Warning: The Database Flashsnap clone database will not be able to be carried over after upgrading. You must create a new Database Flashsnap clone database after upgrading to 6.1.1.

Upgrading SF Oracle RAC and operating system (minor OS upgrade)

This section provides instructions for SF Oracle RAC and minor operating system upgrade.

Perform the steps in the following procedure if you plan to perform a minor upgrade of the operating system, for example from SLES11 SP1 to SLES11 SP2, along with SF Oracle RAC.
Upgrading the operating system

If you want to upgrade the operating system, perform the following steps:

1. Rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:
   ```bash
   # mv /etc/llttab /etc/llttab.save
   ```

2. Upgrade the operating system on all nodes in the cluster.
   For instructions, see the operating system documentation.

   **Note:** If reboot is required, use `shutdown -r now` command to reboot the nodes.

3. After the system restarts, restore the `/etc/llttab` file to its original name:
   ```bash
   # mv /etc/llttab.save /etc/llttab
   ```

### Upgrading SF Oracle RAC using Install Bundles

Use the `installmr` script-based installation programs to upgrade SF Oracle RAC.

The installer performs the following tasks to upgrade SF Oracle RAC:

- Verifies the compatibility of the systems before the upgrade.
- Stops the SF Oracle RAC processes before the upgrade.
- Uninstalls SF Oracle RAC.
- Installs the SF Oracle RAC 6.1 RPMs on the nodes.
- Installs the SF Oracle RAC 6.1.1 patches on the nodes.
- Starts the SF Oracle RAC processes after the upgrade.
- Displays the location of the log files, summary file, and response file.

#### To upgrade to SF Oracle RAC 6.1.1 using the installmr program

1. Log in as superuser.
2. Change to the `/tmp/sfha6.1.1` directory.
3 Invokethe **installmr** script with **-base_path** option to upgrade to 6.1.1:

```
# ./installmr -base_path /tmp/sfha6.1/
```

4 From the opening Selection Menu, choose: **G** for "Upgrade a Product."

5 Select 1 for **Full upgrade**.

The installer displays the copyright message and specifies the directory where the running logs are created.

The installer verifies the systems for compatibility.

---

**Note:** If **had** is stopped before upgrade, the installer displays the following warning:

VCS is not running before upgrade. Please make sure all the configurations are valid before upgrade.

If the configuration files are valid, you may ignore the message.

---

During the system verification phase, the installer checks if the boot disk is encapsulated and the upgrade path. If the upgrade is not supported, you need to un-encapsulate the boot disk.

Review the messages displayed and make sure that you meet the requirements before proceeding with the upgrade.

6 Press **Enter** to continue with the upgrade.

Enter y to agree to the End User License Agreement (EULA).

The installer displays the list of RPMs that will be uninstalled. Press **Enter** to view the list of RPMs that will be upgraded.
7. Enter `y` to stop the SF Oracle RAC processes.

   Do you want to stop SF Oracle RAC processes now? [y,n,q,?] (y)

   The installer stops the processes and uninstalls SF Oracle RAC. After the uninstallation, the installer installs SF Oracle RAC 6.1.1 and starts 6.1.1 on all the nodes.

   If the product is licensed with stale (old) key, the installer prompts users to update the key.

8. Relink the SF Oracle RAC libraries with Oracle:

   The installer prompts a menu after upgrade. If you want the installer to relink the Oracle Database Binary, choose the option **Relink Oracle Database Binary** from the menu.

   Complete the remaining tasks to finish the upgrade.

**Bringing the Oracle database online**

1. Bring the Oracle database service group online.

   - If the Oracle database is managed by VCS:
     
     ```
     # hagr p -online oracle_group -any
     ```

   - If the Oracle database is not managed by VCS:
     
     - For Oracle RAC 11g:
       
       ```
       # srvctl start database -d db_name
       ```

     - For Oracle RAC 12c:
       
       ```
       # srvctl start database -db db_name
       ```

2. Start all applications that are not managed by VCS. Use native application commands to start the applications.

3. If the Oracle database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

   ```
   # haconf -makerw
   # hagr p -modify oracle_group AutoStart 1
   # haconf -dump -makero
   ```
If the Oracle database is not managed by VCS, change the management policy for the database to automatic:

- For Oracle RAC 11g:
  
  $ 
  \texttt{srvctl modify database -d db\_name -y AUTOMATIC} 

- For Oracle RAC 12c:
  
  $ 
  \texttt{srvctl modify database -db db\_name -policy AUTOMATIC} 

4 Complete other post-upgrade steps.

For instructions, see the chapter Performing post-upgrade tasks in Symantec™ Storage Foundation for Oracle RAC 6.1 Installation and Configuration Guide.

5 If you want to upgrade all application clusters to version 6.1.1, make sure that you upgraded CP server systems that use VCS or SFHA to 6.1.1. Then, upgrade all application clusters to version 6.1.1.

For instructions to upgrade VCS or SFHA on the CP server systems, see the 6.1 VCS or SFHA installation guide.

Performing a phased upgrade using Install Bundles

This section explains how to perform a phased upgrade of SFHA Solutions on four nodes with four service groups. Note that in this scenario, SFHA Solutions and the service groups cannot stay online on the second subcluster during the upgrade of the second subcluster. Do not add, remove, or change resources or service groups on any nodes during the upgrade. These changes are likely to get lost after the upgrade.

- Performing a phased VCS upgrade using Install Bundles
- Performing a phased SFHA upgrade using Install Bundles
- Performing a phased SFCFSHA upgrade using Install Bundles
- Performing a phased upgrade of SF Oracle RAC using Install Bundles

Performing a phased VCS upgrade using Install Bundles

You can perform a phased VCS upgrade with the following steps:
Moving the service groups to the second subcluster.
See Veritas Cluster Server 6.0.1 Installation Guide.

2 Upgrading the operating system on the first subcluster.
See Veritas Cluster Server 6.0.1 Installation Guide.

3 Upgrading the first subcluster.
See “Step 3: Upgrading the first subcluster” on page 44.

4 Preparing the second subcluster.
See Veritas Cluster Server 6.0.1 Installation Guide.

5 Activating the first subcluster.
See Veritas Cluster Server 6.0.1 Installation Guide.

6 Upgrading the operating system on the second subcluster.
See Veritas Cluster Server 6.0.1 Installation Guide.

7 Upgrading the second subcluster.
See “Step 7: Upgrading the second subcluster” on page 50.

8 Finishing the phased upgrade.
See Veritas Cluster Server 6.0.1 Installation Guide.

**Moving the service groups to the second subcluster**
Perform the following steps to establish the service group’s status and to switch the service groups.
To move service groups to the second subcluster

1. On the first subcluster, determine where the service groups are online.

   # hagrp -state

   The output resembles:

   # Group  Attribute  System  Value
   sg1  State node01  |ONLINE|
   sg1  State node02  |ONLINE|
   sg1  State node03  |ONLINE|
   sg1  State node04  |ONLINE|
   sg2  State node01  |ONLINE|
   sg2  State node02  |ONLINE|
   sg2  State node03  |ONLINE|
   sg2  State node04  |ONLINE|
   sg3  State node01  |ONLINE|
   sg3  State node02  |ONLINE|
   sg3  State node03  |OFFLINE|
   sg3  State node04  |OFFLINE|
   sg4  State node01  |OFFLINE|
   sg4  State node02  |OFFLINE|
   sg4  State node03  |OFFLINE|
   sg4  State node04  |OFFLINE|

2. Offline the parallel service groups (sg1 and sg2) from the first subcluster. Switch the failover service groups (sg3 and sg4) from the first subcluster (node01 and node02) to the nodes on the second subcluster (node03 and node04). For SFHA, vxfen sg is the parallel service group.

   # hagrp -offline sg1 -sys node01
   # hagrp -offline sg2 -sys node01
   # hagrp -offline sg1 -sys node02
   # hagrp -offline sg2 -sys node02
   # hagrp -switch sg3 -to node03
   # hagrp -switch sg4 -to node04
3 On the nodes in the first subcluster, unmount all the VxFS file systems that VCS does not manage, for example:

```
# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sda1 26G 3.3G 22G 14% /
udev 1007M 352K 1006M 1% /dev
tmpfs 4.0K 0 4.0K 0% /dev/vx
/dev/vx/dsk/dg2/dg2vol1 3.0G 18M 2.8G 1% /mnt/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol2 1.0G 18M 944M 2% /mnt/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol3 10G 20M 9.4G 1% /mnt/dg2/dg2vol3
```

```
# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

4 Make the configuration writable on the first subcluster.

```
# haconf -makerw
```

5 Freeze the nodes in the first subcluster.

```
# hasys -freeze -persistent node01
# hasys -freeze -persistent node02
```

6 Dump the configuration and make it read-only.

```
# haconf -dump -makero
```
7 Verify that the service groups are offline on the first subcluster that you want to upgrade.

```bash
# hagrp -state
```

Output resembles:

```
# Group Attribute System Value
sg1 State node01 | OFFLINE |
sg1 State node02 | OFFLINE |
sg1 State node03 | ONLINE |
sg1 State node04 | ONLINE |
sg2 State node01 | OFFLINE |
sg2 State node02 | OFFLINE |
sg2 State node03 | ONLINE |
sg2 State node04 | ONLINE |
sg3 State node01 | OFFLINE |
sg3 State node02 | OFFLINE |
sg3 State node03 | ONLINE |
sg3 State node04 | OFFLINE |
sg4 State node01 | OFFLINE |
sg4 State node02 | OFFLINE |
sg4 State node03 | OFFLINE |
sg4 State node04 | ONLINE |
```

8 Backup the llttab, llthosts, gabtab, types.cf, main.cf and AT configuration files on the first subcluster.

```bash
# cp /etc/llttab /etc/llttab.bkp
# cp /etc/llthosts /etc/llthosts.bkp
# cp /etc/gabtab /etc/gabtab.bkp
# cp /etc/VRTSvcs/conf/config/main.cf /etc/VRTSvcs/conf/config/main.cf.bkp
# cp /etc/VRTSvcs/conf/config/types.cf /etc/VRTSvcs/conf/config/types.cf.bkp
# /opt/VRTSat/bin/vssat showbackuplist
  /var/VRTSat/.VRTSat/profile/VRTSatlocal.conf
  /var/VRTSat/.VRTSat/profile/certstore
  /var/VRTSat/ABAuthSource
  /etc/vx/vss/VRTSat.conf
Quiescing ...
Snapshot Directory :/var/VRTSatSnapShot
Upgrading the operating system on the first subcluster

You can perform the operating system upgrade on the first subcluster, if required. Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```bash
# mv /etc/llttab /etc/llttab.save
```
or you can change the `/etc/default/llt` file by setting LLT_START = 0.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration. Refer to the operating system’s documentation for more information.

**Step 3: Upgrading the first subcluster**

After step 1 and step 2, you now navigate to the installer program and start it.

**To start the installer for the phased upgrade**

1. Confirm that you are logged on as the superuser and you mounted the product disc.
2. Make sure that you can ssh or rsh from the node where you launched the installer to the nodes in the second subcluster without requests for a password.
3. Start the installvcs program, specify the nodes in the first subcluster (node01 and node02).

```bash
# cd /tmp/sfha6.1.1
# ./installmr -base_path /tmp/sfha6.0.1/ node01 node02
```

The program starts with a copyright message and specifies the directory where it creates the logs.

4. From the opening Selection Menu, choose: **G** for Upgrade a Product.
5. The installer performs a series of checks and tests to ensure communications, licensing, and compatibility.
6. Enter **y** to agree to the End User License Agreement (EULA).
7. The installer displays the list of RPMs that get removed, installed, or upgraded on the selected systems.

8. The installer ends for the first subcluster with the following output:

   Configuring VCS: 100%
   Estimated time remaining: 0:00
   Performing VCS upgrade configuration .................... Done

   Veritas Cluster Server Configure completed successfully

   You are performing phased upgrade (Phase 1) on the systems. Follow the steps in install guide to upgrade the remaining systems.

   Would you like to send the information about this installation to Symantec to help improve installation in the future? [y,n,q,?] (y)

   The upgrade is finished on the first subcluster. Do not reboot the nodes in the first subcluster until you complete the Preparing the second subcluster procedure.

**Preparing the second subcluster**

Perform the following steps on the second subcluster before rebooting nodes in the first subcluster.
To prepare to upgrade the second subcluster

1. Get the summary of the status of your resources.

```bash
# hastatus -sum
-- SYSTEM STATE
-- System   State   Frozen
  A node01   EXITED  1
  A node02   EXITED  1
  A node03   RUNNING 0
  A node04   RUNNING 0

-- GROUP STATE
-- Group   System   Probed   AutoDisabled   State
  B sg1     node01   Y       N             OFFLINE
  B sg1     node02   Y       N             OFFLINE
  B sg1     node03   Y       N             ONLINE
  B sg1     node04   Y       N             ONLINE
  B sg2     node01   Y       N             OFFLINE
  B sg2     node02   Y       N             OFFLINE
  B sg2     node03   Y       N             ONLINE
  B sg2     node04   Y       N             ONLINE
  B sg3     node01   Y       N             OFFLINE
  B sg3     node02   Y       N             OFFLINE
  B sg3     node03   Y       N             ONLINE
  B sg3     node04   Y       N             OFFLINE
  B sg4     node01   Y       N             OFFLINE
  B sg4     node02   Y       N             OFFLINE
  B sg4     node03   Y       N             OFFLINE
  B sg4     node04   Y       N             ONLINE
```
2 Unmount all the VxFS file systems that VCS does not manage, for example:

```
# df -h
Filesystem     Size  Used  Avail  Use% Mounted on
/dev/sda1      26G   3.3G   22G   14% /    
udev           1007M  352K  1006M   1% /dev
tmpfs          4.0K   0     4.0K   0% /dev/vx
/dev/vx/dsk/dg2/dg2vol1  3.0G  18M  2.8G   1% /mnt/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol2  1.0G  18M  944M   2% /mnt/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol3 10G  20M  9.4G   1% /mnt/dg2/dg2vol3
# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

3 Make the configuration writable on the second subcluster.

```
# haconf -makerw
```

4 Unfreeze the service groups.

```
# hagrp -unfreeze sg1 -persistent
# hagrp -unfreeze sg2 -persistent
# hagrp -unfreeze sg3 -persistent
# hagrp -unfreeze sg4 -persistent
```

5 Dump the configuration and make it read-only.

```
# haconf -dump -makero
```

6 Take the service groups offline on node03 and node04.

```
# hagrp -offline sg1 -sys node03
# hagrp -offline sg1 -sys node04
# hagrp -offline sg2 -sys node03
# hagrp -offline sg2 -sys node04
# hagrp -offline sg3 -sys node03
# hagrp -offline sg4 -sys node04
```

Upgrading to 6.1.1 from releases earlier than 6.1
Performing a phased upgrade using Install Bundles
7  Verify the state of the service groups.

   # hagrp -state
   #Group   Attribute System  Value
   sg1      State    node01 |OFFLINE|
   sg1      State    node02 |OFFLINE|
   sg1      State    node03 |OFFLINE|
   sg1      State    node04 |OFFLINE|
   sg2      State    node01 |OFFLINE|
   sg2      State    node02 |OFFLINE|
   sg2      State    node03 |OFFLINE|
   sg2      State    node04 |OFFLINE|
   sg3      State    node01 |OFFLINE|
   sg3      State    node02 |OFFLINE|
   sg3      State    node03 |OFFLINE|
   sg3      State    node04 |OFFLINE|

8  Stop VCS, I/O Fencing, GAB, and LLT on node03 and node04.

   # hastop -local
   # /etc/init.d/vxfen stop
   # /etc/init.d/gab stop
   # /etc/init.d/llt stop

9  Make sure that the VXFEN, GAB, and LLT modules on node03 and node04 are not added.

   # /etc/init.d/vxfen status
   VXFEN module is not loaded

   # /etc/init.d/gab status
   GAB module is not loaded

   # /etc/init.d/llt status
   LLT module is not loaded

Activating the first subcluster
Get the first subcluster ready for the service groups.

Note: These steps fulfill part of the installer's output instructions, see Step 3: Upgrading the first subcluster step Preparing the second subcluster.
To activate the first subcluster

1. Start LLT and GAB.
   
   ```
   # /etc/init.d/llt start
   # /etc/init.d/gab start
   ```

2. Seed node01 and node02 in the first subcluster.
   
   ```
   # gabconfig -x
   ```

3. On the first half of the cluster, start VCS:
   
   ```
   # cd /opt/VRTS/install
   # ./installvcs<version> -start node01 node02
   ```
   Where `<version>` is the specific release version.

4. Make the configuration writable on the first subcluster.
   
   ```
   # haconf -makerw
   ```

5. Unfreeze the nodes in the first subcluster.
   
   ```
   # hasys -unfreeze -persistent node01
   # hasys -unfreeze -persistent node02
   ```

6. Unfreeze service groups in the first subcluster.
   
   ```
   # hagrp -unfreeze sg1 -persistent
   # hagrp -unfreeze sg2 -persistent
   ```

7. Dump the configuration and make it read-only.
   
   ```
   # haconf -dump -makero
   ```

8. Bring the service groups online on node01 and node02.
   
   ```
   # hagrp -online sg1 -sys node01
   # hagrp -online sg1 -sys node02
   # hagrp -online sg2 -sys node01
   # hagrp -online sg2 -sys node02
   # hagrp -online sg3 -sys node01
   # hagrp -online sg4 -sys node02
   ```
Upgrading the operating system on the second subcluster

You can perform the operating system upgrade on the second subcluster, if required.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting `LLT_START = 0`.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system’s documentation for more information.

Step 7: Upgrading the second subcluster

After step 4 to step 6, perform the following procedure to upgrade the second subcluster (node03 and node04).

To start the installer to upgrade the second subcluster

1. Confirm that you are logged on as the superuser and you mounted the product disc.

2. Navigate to the folder that contains the SFHA Solutions 6.1.1 binary.

   ```
   # cd /tmp/sfha6.1.1
   ```

3. Confirm that VCS is stopped on node03 and node04. Specify the nodes in the second subcluster (node03 and node04).

   ```
   # ./installmr -base_path /tmp/sfha6.0.1/ node03 node04
   ```

   The program starts with a copyright message and specifies the directory where it creates the logs.

4. From the opening Selection Menu, choose: G for Upgrade a Product.

5. The installer performs a series of checks and tests to ensure communications, licensing, and compatibility.

6. Enter y to agree to the End User License Agreement (EULA).

7. The installer displays the list of RPMs that get removed, installed, or upgraded on the selected systems.

8. Monitor the installer program answering questions as appropriate until the upgrade completes.
Finishing the phased upgrade

Complete the following procedure to complete the upgrade.

To finish the upgrade

1. Verify that the cluster UUID is the same on the nodes in the second subcluster and the first subcluster. Run the following command to display the cluster UUID:

   ```
   # /opt/VRTSvcs/bin/uuidconfig.pl
   -clus -display node01 [node02 ...]
   ```

   If the cluster UUID differs, manually copy the cluster UUID from a node in the first subcluster to the nodes in the second subcluster. For example:

   ```
   # /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus
   -copy -from_sys node01 -to_sys node03 node04
   ```

2. On the second half of the cluster, start VCS:

   ```
   # cd /opt/VRTS/install
   # ./installvcs<version> -start node03 node04
   ```

   Where `<version>` is the specific release version.
3 Check to see if VCS and its components are up.

```bash
# gabconfig -a
```

GAB Port Memberships

```
Port a gen nxxxnn membership 0123
Port b gen nxxxnn membership 0123
Port h gen nxxxnn membership 0123
```

4 Run an `hastatus -sum` command to determine the status of the nodes, service groups, and cluster.

```bash
# hastatus -sum
```

<table>
<thead>
<tr>
<th>-- SYSTEM STATE</th>
<th>State</th>
<th>Frozen</th>
</tr>
</thead>
<tbody>
<tr>
<td>A node01</td>
<td>RUNNING</td>
<td>0</td>
</tr>
<tr>
<td>A node02</td>
<td>RUNNING</td>
<td>0</td>
</tr>
<tr>
<td>A node03</td>
<td>RUNNING</td>
<td>0</td>
</tr>
<tr>
<td>A node04</td>
<td>RUNNING</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>-- GROUP STATE</th>
<th>System</th>
<th>Probed</th>
<th>AutoDisabled</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>B sg1 node01</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg1 node02</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg1 node03</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg1 node04</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg2 node01</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg2 node02</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg2 node03</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg2 node04</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg3 node01</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg3 node02</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg3 node03</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg3 node04</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg4 node01</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg4 node02</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg4 node03</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg4 node04</td>
<td>Y</td>
<td>N</td>
<td></td>
<td>OFFLINE</td>
</tr>
</tbody>
</table>
In this example, you have performed a phased upgrade of VCS. The service groups were down when you took them offline on node03 and node04, to the time VCS brought them online on node01 and node02.

**Note:** If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA, see the VCS or SFHA Installation Guide.

### Performing a phased SFHA upgrade using Install Bundles

You can perform a phased upgrade from SFHA 5.0 MP3 or other supported previous versions to SFHA 6.1.1.

Performing a phased upgrade involves the following tasks:

1. Moving the service groups to the second subcluster.
   - See *Veritas Storage Foundation and High Availability 6.0.1 Installation Guide*.

2. Upgrading the operating system on the first subcluster.
   - See *Veritas Storage Foundation and High Availability 6.0.1 Installation Guide*.

3. Upgrading the first subcluster.
   - See “Upgrading the first subcluster” on page 58.

4. Preparing the second subcluster.
   - See *Veritas Storage Foundation and High Availability 6.0.1 Installation Guide*.

5. Activating the first subcluster.
   - See *Veritas Storage Foundation and High Availability 6.0.1 Installation Guide*.

6. Upgrading the operating system on the second subcluster.
   - See *Veritas Storage Foundation and High Availability 6.0.1 Installation Guide*. 
7 Upgrading the second subcluster.
   See “Upgrading the second subcluster” on page 64.

8 Finishing the phased upgrade.
   See Veritas Storage Foundation and High Availability 6.0.1 Installation Guide.

Moving the service groups to the second subcluster

Perform the following steps to establish the service group's status and to switch the service groups.
To move service groups to the second subcluster

1. On the first subcluster, determine where the service groups are online.

   # hagrp -state

   The output resembles:

   # Group | Attribute | System | Value
   --- | --- | --- | ---
   sg1 | State | node01 | ONLINE
   sg1 | State | node02 | ONLINE
   sg1 | State | node03 | ONLINE
   sg1 | State | node04 | ONLINE
   sg2 | State | node01 | ONLINE
   sg2 | State | node02 | ONLINE
   sg2 | State | node03 | ONLINE
   sg2 | State | node04 | ONLINE
   sg3 | State | node01 | ONLINE
   sg3 | State | node02 | ONLINE
   sg3 | State | node03 | OFFLINE
   sg3 | State | node04 | OFFLINE
   sg4 | State | node01 | OFFLINE
   sg4 | State | node02 | OFFLINE
   sg4 | State | node03 | OFFLINE
   sg4 | State | node04 | OFFLINE

2. Offline the parallel service groups (sg1 and sg2) from the first subcluster. Switch the failover service groups (sg3 and sg4) from the first subcluster (node01 and node02) to the nodes on the second subcluster (node03 and node04). For SFHA, vxfen sg is the parallel service group.

   # hagrp -offline sg1 -sys node01
   # hagrp -offline sg2 -sys node01
   # hagrp -offline sg1 -sys node02
   # hagrp -offline sg2 -sys node02
   # hagrp -switch sg3 -to node03
   # hagrp -switch sg4 -to node04
3 On the nodes in the first subcluster, unmount all the VxFS file systems that VCS does not manage, for example:

```bash
# df -h
Filesystem  Size  Used  Avail  Use% Mounted on
/dev/sda1    26G   3.3G   22G   14% /
udev         1007M 352K  1006M   1% /dev
tmpfs        4.0K   0   4.0K   0% /dev/vx
/dev/vx/dsk/dg2/dg2vol1
            3.0G  18M   2.8G   1% /mnt/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol2
            1.0G  18M   944M   2% /mnt/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol3
            10G  20M   9.4G   1% /mnt/dg2/dg2vol3
# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

4 On the nodes in the first subcluster, stop all VxVM volumes (for each disk group) that VCS does not manage.

5 Make the configuration writable on the first subcluster.

```bash
# haconf -makerw
```

6 Freeze the nodes in the first subcluster.

```bash
# hasys -freeze -persistent node01
# hasys -freeze -persistent node02
```

7 Dump the configuration and make it read-only.

```bash
# haconf -dump -makero
```
8 Verify that the service groups are offline on the first subcluster that you want to upgrade.

```
# hagrp -state
```

Output resembles:

```
#Group Attribute System Value
sg1  State node01 |OFFLINE|
sg1  State node02 |OFFLINE|
sg1  State node03 |ONLINE|
sg1  State node04 |ONLINE|
sg2  State node01 |OFFLINE|
sg2  State node02 |OFFLINE|
sg2  State node03 |ONLINE|
sg2  State node04 |ONLINE|
sg3  State node01 |OFFLINE|
sg3  State node02 |OFFLINE|
sg3  State node03 |ONLINE|
sg3  State node04 |OFFLINE|
sg4  State node01 |OFFLINE|
sg4  State node02 |OFFLINE|
sg4  State node03 |OFFLINE|
sg4  State node04 |ONLINE|
```

9 Back up the llttab, llthosts, gabtab, types.cf, main.cf and AT configuration files on the first subcluster.

```
# cp /etc/llttab /etc/llttab.bkp
# cp /etc/llthosts /etc/llthosts.bkp
# cp /etc/gabtab /etc/gabtab.bkp
# cp /etc/VRTSvcs/conf/config/main.cf /etc/VRTSvcs/conf/config/main.cf.bkp
# cp /etc/VRTSvcs/conf/config/types.cf /etc/VRTSvcs/conf/config/types.cf.bkp
# /opt/VRTSat/bin/vssat showbackuplist
B|/var/VRTSat/.VRTSat/profile/VRTSatlocal.conf
B|/var/VRTSat/.VRTSat/profile/certstore
B|/var/VRTSat/ABAuthSource
B|/etc/vx/vss/VRTSat.conf
Quiescing ...
Snapshot Directory :/var/VRTSatSnapShot
Upgrading the operating system on the first subcluster

You can perform the operating system upgrade on the first subcluster, if required. Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```bash
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting LLT_START = 0.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system’s documentation for more information.

Upgrading the first subcluster

After step 1 and step 2, you now navigate to the installer program and start it.

To start the installer for the phased upgrade

1. Confirm that you are logged on as the superuser and you mounted the product disc.

2. Navigate to the folder that contains the SFHA Solutions 6.1.1 binary.

   ```bash
   # cd /tmp/sfha6.1.1.
   ```

3. Make sure that you can ssh or rsh from the node where you launched the installer to the nodes in the second subcluster without requests for a password.

4. Start the installmr program, specify the nodes in the first subcluster (node01 and node02).

   ```bash
   # ./installmr -base_path /tmp/sfha6.0.1/ node01 node02
   ```

   The program starts with a copyright message and specifies the directory where it creates the logs. It performs a system verification and outputs upgrade information.

5. From the opening Selection Menu, select G for Upgrade a Product and from the sub menu, select Full Upgrade.

6. Enter y to agree to the End User License Agreement (EULA).
7 The installer displays the list of RPMs that get removed, installed, and upgraded on the selected systems.

8 When you are prompted, reply \texttt{y} to stop appropriate processes.

Do you want to stop SFHA processes now? [y,n,q] (y)

The installer stops processes, uninstalls RPMs, and installs RPMs.

The upgrade is finished on the first subcluster. Do not reboot the nodes in the first subcluster until you complete the \textit{Upgrading the second subcluster} procedure.

**Preparing the second subcluster**

Perform the following steps on the second subcluster before rebooting nodes in the first subcluster.
To prepare to upgrade the second subcluster

1. Get the summary of the status of your resources.

```
# hastatus -sum

-- SYSTEM STATE

<table>
<thead>
<tr>
<th>System</th>
<th>State</th>
<th>Frozen</th>
</tr>
</thead>
<tbody>
<tr>
<td>A node01</td>
<td>EXITED</td>
<td>1</td>
</tr>
<tr>
<td>A node02</td>
<td>EXITED</td>
<td>1</td>
</tr>
<tr>
<td>A node03</td>
<td>RUNNING</td>
<td>0</td>
</tr>
<tr>
<td>A node04</td>
<td>RUNNING</td>
<td>0</td>
</tr>
</tbody>
</table>

-- GROUP STATE

<table>
<thead>
<tr>
<th>Group</th>
<th>System</th>
<th>Probed</th>
<th>AutoDisabled</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>B sg1</td>
<td>node01</td>
<td>Y</td>
<td>N</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg1</td>
<td>node02</td>
<td>Y</td>
<td>N</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg1</td>
<td>node03</td>
<td>Y</td>
<td>N</td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg1</td>
<td>node04</td>
<td>Y</td>
<td>N</td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg2</td>
<td>node01</td>
<td>Y</td>
<td>N</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg2</td>
<td>node02</td>
<td>Y</td>
<td>N</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg2</td>
<td>node03</td>
<td>Y</td>
<td>N</td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg2</td>
<td>node04</td>
<td>Y</td>
<td>N</td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg3</td>
<td>node01</td>
<td>Y</td>
<td>N</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg3</td>
<td>node02</td>
<td>Y</td>
<td>N</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg3</td>
<td>node03</td>
<td>Y</td>
<td>N</td>
<td>ONLINE</td>
</tr>
<tr>
<td>B sg3</td>
<td>node04</td>
<td>Y</td>
<td>N</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg4</td>
<td>node01</td>
<td>Y</td>
<td>N</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg4</td>
<td>node02</td>
<td>Y</td>
<td>N</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg4</td>
<td>node03</td>
<td>Y</td>
<td>N</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>B sg4</td>
<td>node04</td>
<td>Y</td>
<td>N</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>
```

Performing a phased upgrade using Install Bundles.
2 Unmount all the VxFS file systems that VCS does not manage, for example:

```bash
# df -h
Filesystem      Size  Used  Avail  Use% Mounted on
/dev/sda1       26G   3.3G   22G   14%   /
udev             1007M 352K 1006M   1%  /dev
/tmpfs           4.0K   0   4.0K   0%  /dev/vx
/dev/vx/dsk/dg2/dg2vol1 3.0G  18M  2.8G   1%  /mnt/dg2/dg2vol1
/dev/vx/dsk/dg2/dg2vol2 1.0G  18M  944M   2%  /mnt/dg2/dg2vol2
/dev/vx/dsk/dg2/dg2vol3 10G  20M  9.4G   1%  /mnt/dg2/dg2vol3
```

```bash
# umount /mnt/dg2/dg2vol1
# umount /mnt/dg2/dg2vol2
# umount /mnt/dg2/dg2vol3
```

3 Make the configuration writable on the second subcluster.

```bash
# haconf -makerw
```

4 Unfreeze the service groups.

```bash
# hagrp -unfreeze sg1 -persistent
# hagrp -unfreeze sg2 -persistent
# hagrp -unfreeze sg3 -persistent
# hagrp -unfreeze sg4 -persistent
```

5 Dump the configuration and make it read-only.

```bash
# haconf -dump -makero
```

6 Take the service groups offline on node03 and node04.

```bash
# hagrp -offline sg1 -sys node03
# hagrp -offline sg1 -sys node04
# hagrp -offline sg2 -sys node03
# hagrp -offline sg2 -sys node04
# hagrp -offline sg3 -sys node03
# hagrp -offline sg4 -sys node04
```
7 Verify the state of the service groups.

```
# hagrp -state
# Group  Attribute  System   Value
sg1    State      node01   |OFFLINE|
sg1    State      node02   |OFFLINE|
sg1    State      node03   |OFFLINE|
sg1    State      node04   |OFFLINE|
sg2    State      node01   |OFFLINE|
sg2    State      node02   |OFFLINE|
sg2    State      node03   |OFFLINE|
sg2    State      node04   |OFFLINE|
sg3    State      node01   |OFFLINE|
sg3    State      node02   |OFFLINE|
sg3    State      node03   |OFFLINE|
sg3    State      node04   |OFFLINE|
```

8 Stop all VxVM volumes (for each disk group) that VCS does not manage.

9 Stop VCS, I/O Fencing, GAB, and LLT on node03 and node04.

```
# hastop -local
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

10 Make sure that the VXFEN, GAB, and LLT modules on node03 and node04 are not added.

```
# /etc/init.d/vxfen status
VXFEN module is not loaded

# /etc/init.d/gab status
GAB module is not loaded

# /etc/init.d/llt status
LLT module is not loaded
```

Activating the first subcluster

Get the first subcluster ready for the service groups.
To activate the first subcluster
1  Start LLT and GAB.
   # /etc/init.d/llt start
   # /etc/init.d/gab start

2  Seed node01 and node02 in the first subcluster.
   # gabconfig -x

3  If the product doesn't start automatically, on the first half of the cluster, start SFHA:
   # cd /opt/VRTS/install
   # ./installsfha<version> -start node01 node02
   Where <version> is the specific release version.

4  Make the configuration writable on the first subcluster.
   # haconf -makerw

5  Unfreeze the nodes in the first subcluster.
   # hasys -unfreeze -persistent node01
   # hasys -unfreeze -persistent node02

6  Unfreeze service groups in the first subcluster:
   # hagrp -unfreeze sg1 -persistent
   # hagrp -unfreeze sg2 -persistent
7. Dump the configuration and make it read-only.

```bash
# haconf -dump -makero
```

8. Bring the service groups online on node01 and node02.

```bash
# hagrp -online sg1 -sys node01
# hagrp -online sg1 -sys node02
# hagrp -online sg2 -sys node01
# hagrp -online sg2 -sys node02
# hagrp -online sg3 -sys node01
# hagrp -online sg4 -sys node02
```

**Upgrading the operating system on the second subcluster**

You can perform the operating system upgrade on the second subcluster, if required. Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```bash
# mv /etc/llttab /etc/llttab.save
```

or you can change the `/etc/default/llt` file by setting `LLT_START = 0`.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system’s documentation for more information.

**Upgrading the second subcluster**

After step 4 to step 6, perform the following procedure to upgrade the second subcluster (node03 and node04).

**To start the installer to upgrade the second subcluster**

1. Confirm that you are logged on as the superuser and you mounted the product disc.

2. Navigate to the folder that contains the SFHA Solutions 6.1.1 binary.

```bash
# cd /tmp/sfha6.1.1.
```
3 Confirm that SFHA is stopped on node03 and node04. Start the installmr program, specify the nodes in the second subcluster (node03 and node04).

```bash
# ./installmr -base_path /tmp/sfha6.0.1/ node03 node04
```

The program starts with a copyright message and specifies the directory where it creates the logs.

4 From the opening Selection Menu, select G for **Upgrade a Product** and from the sub menu, select **Full Upgrade**.

5 The installer displays the list of RPMs that get removed, installed, and upgraded on the selected systems.

6 When you are prompted, reply `y` to stop appropriate processes.

```
Do you want to stop SFHA processes now? [y,n,q] (y)
```

The installer stops processes, uninstalls RPMs, and installs RPMs.

7 Enter `y` to agree to the End User License Agreement (EULA).

8 Monitor the installer program answering questions as appropriate until the upgrade completes.

```
After this step, for finishing the phased upgrade, see Veritas Storage Foundation and High Availability 6.0.1 Installation Guide.
```

**Finishing the phased upgrade**

Complete the following procedure to complete the upgrade.
To finish the upgrade

1. Verify that the cluster UUID is the same on the nodes in the second subcluster and the first subcluster. Run the following command to display the cluster UUID:

```bash
# /opt/VRTSvcs/bin/uuidconfig.pl 
-clus -display node01 [node02 ...]
```

If the cluster UUID differs, manually copy the cluster UUID from a node in the first subcluster to the nodes in the second subcluster. For example:

```bash
# /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus 
-copy -from_sys node01 -to_sys node03 node04
```

2. On the second half of the cluster, start SFHA:

```bash
# cd /opt/VRTS/install
# ./installsfha<version> -start node03 node04
```

Where `<version>` is the specific release version.

3. Check to see if SFHA and its components are up.

```bash
# gabconfig -a
```

GAB Port Memberships

```
GAB Port Memberships
=======

Port a gen  nxxxnn membership 0123
Port b gen  nxxxxn membership 0123
Port h gen  nxxxxn membership 0123
```
4 Run an `hastatus -sum` command to determine the status of the nodes, service groups, and cluster.

```bash
# hastatus -sum

-- SYSTEM STATE
-- System State Frozen
A  node01 RUNNING 0
A  node02 RUNNING 0
A  node03 RUNNING 0
A  node04 RUNNING 0

-- GROUP STATE
-- Group System Probed AutoDisabled State
B sg1 node01 Y N ONLINE
B sg1 node02 Y N ONLINE
B sg1 node03 Y N ONLINE
B sg1 node04 Y N ONLINE
B sg2 node01 Y N ONLINE
B sg2 node02 Y N ONLINE
B sg2 node03 Y N OFFLINE
B sg2 node04 Y N OFFLINE
B sg3 node01 Y N ONLINE
B sg3 node02 Y N OFFLINE
B sg3 node03 Y N OFFLINE
B sg3 node04 Y N OFFLINE
B sg4 node01 Y N OFFLINE
B sg4 node02 Y N ONLINE
B sg4 node03 Y N OFFLINE
B sg4 node04 Y N OFFLINE
```

5 After the upgrade is complete, start the VxVM volumes (for each disk group) and mount the VxFS file systems.

In this example, you have performed a phased upgrade of SFHA. The service groups were down when you took them offline on node03 and node04, to the time SFHA brought them online on node01 or node02.
Performing a phased SFCFSHA upgrade using Install Bundles

Performing a phased upgrade involves the following tasks:

1. Moving the service groups to the second subcluster.
   See *Veritas Storage Foundation Cluster File System High Availability 6.0.1 Installation Guide*.

2. Upgrading the SFCFSHA stack on the first subcluster.
   See "Upgrading the SFCFSHA stack on the first subcluster" on page 70.

3. Preparing the second subcluster.
   See *Veritas Storage Foundation Cluster File System High Availability 6.0.1 Installation Guide*.

4. Activating the first subcluster.
   See *Veritas Storage Foundation Cluster File System High Availability 6.0.1 Installation Guide*.

5. Upgrading the operating system on the second subcluster.
   See *Veritas Storage Foundation Cluster File System High Availability 6.0.1 Installation Guide*.

6. Upgrading the second subcluster.
   See "Upgrading the second subcluster" on page 74.

7. Completing the phased upgrade.

Before you start the upgrade on the first half of the cluster, back up the VCS configuration files `main.cf` and `types.cf` which are in the directory `/etc/VRTSvcs/conf/config/`.

**Note:** If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA, see the VCS or SFHA Installation Guide.
Moving the service groups to the second subcluster

To move the service groups to the second subcluster

1 Switch failover groups from the first half of the cluster to one of the nodes in the second half of the cluster. In this procedure, node01 is a node in the first half of the cluster and node04 is a node in the second half of the cluster. Enter the following:

```bash
# hagrp -switch failover_group -to node04
```

2 On the first half of the cluster, stop all applications that are not configured under VCS. Use native application commands to stop the applications.

3 On the first half of the cluster, unmount the VxFS or CFS file systems that are not managed by VCS.

```bash
# mount | grep vxfs
```

Verify that no processes use the VxFS or CFS mount point. Enter the following:

```bash
# fuser -c /mount_point
```

Stop any processes using a VxFS or CFS mount point with the mechanism provided by the application.

Unmount the VxFS or CFS file system. Enter the following:

```bash
# umount /mount_point
```

4 On the first half of the cluster, bring all the VCS service groups offline including CVM group. Enter the following:

```bash
# hagrp -offline group_name -sys node01
```

When the CVM group becomes OFFLINE, all the parallel service groups such as the CFS file system will also become OFFLINE on the first half of the cluster nodes.

5 Verify that the VCS service groups are offline on all the nodes in first half of the cluster. Enter the following:

```bash
# hagrp -state group_name
```

6 Freeze the nodes in the first half of the cluster. Enter the following:

```bash
# haconf -makerw
# hasys -freeze -persistent node01
# haconf -dump -makero
```
7 Verify that only GAB ports a, b, d and h are open. Enter the following:

```
# gabconfig -a
```

GAB Port Memberships
======================================================================
Port a gen 6b5901 membership 01
Port b gen 6b5904 membership 01
Port d gen 6b5907 membership 01
Port h gen ada40f membership 01

Do not stop VCS. Port h should be up and running.

8 In the first half of the cluster, stop all VxVM and CVM volumes. Enter the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open. Enter the following:

```
# vxprint -Aht -e v_open
```

9 On first half of the cluster, upgrade the operating system on all the nodes, if applicable. For instructions, see the upgrade paths for the operating system.

When the node starts, prevent LLT from starting automatically with one of the following methods. For example, . Or, change the /etc/default/llt file by setting LLT_START = 0. After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

- Enter:

```
# mv /etc/llttab /etc/llttab.save
```

OR:

- Set LLT_START = 0 in the /etc/default/llt file

---

**Note:** After upgrading the OS, change the LLT configuration to its original configuration.

---

**Upgrading the SFCFSHA stack on the first subcluster**

After step 1, you now navigate to the installer program and start it.
To upgrade the SFCFSHA stack on the first subcluster

1. **Note:** This procedure is based on an "in-place" upgrade path; that is, if the operating system is upgraded, the release will be the same, but only the path level will change. If you are moving from major operating system release to another, you must uninstall the SFCFSHA stack before you upgrade the operating system. After the operating system is upgraded, you must reinstall SFCFSHA.

On the first half of the cluster, upgrade SFCFSHA by using the installmr script. For example use the installmr script with Install Bundles as shown below:

```
# ./installmr -base_path /tmp/sfha6.0.1/ node01
```

where `<node01>` is the node on the first subcluster.

**Note:** Do not reboot the nodes in the first subcluster until you complete the Preparing the second subcluster procedure.

After the upgrade for first half of the cluster is complete, no GAB ports will be shown in `gabconfig -a` output.

2. From the opening Selection Menu, choose: G for **Upgrade a Product**.
Preparing the second subcluster

To prepare the second subcluster

1. On the second half of the cluster, stop all applications that are not configured under VCS. Use native application commands to stop the application. [Downtime starts now.]

2. On the second half of the cluster, unmount the VxFS and CFS file systems that are not managed by VCS. Enter the following:

   ```
   # mount | grep vxfs
   ```

   Verify that no processes use the VxFS and CFS mount point. Enter the following:

   ```
   # fuser -c /mount_point
   ```

   Stop any processes using a VxFS and CFS mount point with the mechanism provided by the application.

   Unmount the VxFS and CFS file system. Enter the following:

   ```
   # umount /mount_point
   ```

3. On the second half of the cluster, unfreeze all the VCS service groups on all the nodes using the following commands:

   ```
   # haconf -makerw
   # hagrp -unfreeze group_name -persistent
   # haconf -dump -makero
   ```

4. On the second half of the cluster, bring all the VCS service groups offline, including CVM group. Enter the following:

   ```
   # hagrp -offline group_name -sys node04
   ```

5. On the second half of the cluster, verify that the VCS service groups are offline. Enter the following:

   ```
   # hagrp -state group_name
   ```
6  Stop VCS on the second half of the cluster. Enter the following:

```
# hastop -local
```

7  On the second half of the cluster, stop the following SFCFSHA modules: GLM, ODM, GMS, VxFEN, GAB, and LLT. Enter the following:

```
# /etc/init.d/vxglm stop
# /etc/init.d/vxodm stop
# /etc/init.d/vxgms stop
# /etc/init.d/vxfen stop
# /etc/init.d/gab stop
# /etc/init.d/llt stop
```

**Activating the first subcluster**

To activate the first subcluster

1  Start LLT and GAB:

```
# /etc/init.d/llt start
# /etc/init.d/gab start
```

2  Force GAB to form a cluster in the first half of the cluster.

```
# /sbin/gabconfig -x
```

GAB port a appear in `gabconfig -a` command output.

3  If the product doesn’t start automatically, on the first half of the cluster, start SFCFSHA:

```
# cd /opt/VRTS/install
# ./installsfcfsha<version> -start node01 node02
```

Where `<version>` is the specific release version.

4  Unfreeze the nodes in the first half of the cluster. Enter the following:

```
# haconf -makerw
# hasys -unfreeze -persistent node_name
# haconf -dump -makero
```
5 On the first half of the cluster, bring the VCS service groups online. Enter the following:

```
# hagrp -online group_name -sys node_name
```

After you bring the CVM service group ONLINE, all the GAB ports u, v, w and f come ONLINE and all the CFS mounts service groups also come ONLINE automatically. Only failover service groups need to be brought ONLINE manually.

6 Manually mount the VxFS and CFS file systems that are not managed by VCS. [Downtime ends now.]

**Upgrading the operating system on the second subcluster**

You can perform the operating system upgrade on the second subcluster, if required.

Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:

```
# mv /etc/llttab /etc/llttab.save
```

or you can change the /etc/default/llt file by setting LLT_START = 0.

After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.

Refer to the operating system’s documentation for more information.

**Upgrading the second subcluster**

After step 3 to step 5, upgrade the second subcluster.

**To upgrade the second subcluster**

1 Enter the following:

```
# ./installmr -base_path /tmp/sfha6.0.1/ node_name
```

2 From the opening Selection Menu, choose: G for **Upgrade a Product**.
**Finishing the phased upgrade**

To finish the phased upgrade

1. Verify that the cluster UUID on the nodes in the second subcluster is the same as the cluster UUID on the nodes in the first subcluster. Run the following command to display the cluster UUID:

   ```bash
   # /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus -display nodename
   ```

   If the cluster UUID differs, manually copy the cluster UUID from a node in the first subcluster to the nodes in the second subcluster. For example:

   ```bash
   # /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus -copy -from_sys \node01 -to_sys node03 node04
   ```

2. Run the installer to start SFCFSHA on the second subcluster:

   ```bash
   # ./opt/VRTS/install/installsfcfsha61 node03 node04
   ```

3. Manually mount the VxFS and CFS file systems that are not managed by VCS in the second half of the cluster.

4. Find out which node is the CVM master. Enter the following:

   ```bash
   # vxdctl -c mode
   ```

5. On the CVM master node, upgrade the CVM protocol. Enter the following:

   ```bash
   # vxdctl upgrade
   ```

**Performing a phased upgrade of SF Oracle RAC using Install Bundles**

The phased upgrade methodology involves upgrading half of the nodes in the cluster at a time. The procedure involves the following tasks:

1. Performing pre-upgrade tasks on the first half of the cluster.
   
   See “Step 1: Performing pre-upgrade tasks on the first half of the cluster” on page 76.

2. Upgrading the first half of the cluster.

   **Step 2: Upgrading the first half of the cluster**

3. Performing pre-upgrade tasks on the second half of the cluster.

   See “Step 3: Performing pre-upgrade tasks on the second half of the cluster” on page 80.
Performing post-upgrade tasks on the first half of the cluster.

Step 4: Performing post-upgrade tasks on the first half of the cluster

Upgrading the second half of the cluster.

Step 5: Upgrading the second half of the cluster

Performing post-upgrade tasks on the second half of the cluster.

Step 6: Performing post-upgrade tasks on the second half of the cluster

Step 1: Performing pre-upgrade tasks on the first half of the cluster

Perform the following pre-upgrade steps on the first half of the cluster.

To perform the pre-upgrade tasks on the first half of the cluster

1. Back up the following configuration files: main.cf, types.cf, CVMTypes.cf, CFSTypes.cf, OracleTypes.cf, OracleASMTypes.cf, PrivNIC.cf, MultiPrivNIC.cf, /etc/llttab, /etc/llthosts, /etc/gabtab, /etc/vxfentab, /etc/vxfendg, /etc/vxfenmode

   For example:

   ```
   # cp /etc/VRTSvcs/conf/config/main.cf   
   /etc/VRTSvcs/conf/config/main.cf.save
   # cp /etc/VRTSvcs/conf/config/types.cf   
   /etc/VRTSvcs/conf/config/types.cf.save
   # cp /etc/VRTSvcs/conf/config/OracleTypes.cf  
   /etc/VRTSvcs/conf/config/OracleTypes.cf.save
   # cp /etc/VRTSvcs/conf/config/PrivNIC.cf  
   /etc/VRTSvcs/conf/config/PrivNIC.cf.save
   # cp /etc/VRTSvcs/conf/config/MultiPrivNIC.cf  
   /etc/VRTSvcs/conf/config/MultiPrivNIC.cf.save
   
   The installer verifies that recent backups of configuration files in the VxVM private region are saved in /etc/vx/cbr/bk.

   If not, the following warning message is displayed: Warning: Backup /etc/vx/cbr/bk directory.

2. Stop all applications that are not configured under VCS but dependent on Oracle RAC or resources controlled by VCS. Use native application commands to stop the application.

3. Stop the applications configured under VCS. Stop the Oracle database:
   - If the Oracle RAC instance is managed by VCS:
If the Oracle RAC instance is not managed by VCS, log in as the Oracle user on one of the nodes in the first half of the cluster and shut down the instances:

For Oracle RAC 12c:

```
$ srvctl stop instance -db db_name \
   -node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl stop instance -d db_name \
   -n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl stop instance -d db_name \
   -i instance_name
```

If the Oracle database is managed by VCS, set the AutoStart value to 0 to prevent the database service group from starting automatically when VCS starts:

```
# haconf -makerw 
# hagrp -modify oracle_group AutoStart 0 
# haconf -dump -makero
```

If the Oracle database is not managed by VCS, change the management policy for the database to manual:

For Oracle 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y MANUAL
```

Unmount the CFS file systems that are not managed by VCS.

Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the CFS mount point:

```
# mount | grep vxfs | grep cluster
```
# fuser -cu /mount_point

- Unmount the CFS file system:
  
  ```
  # umount /mount_point
  ```

6 Stop the parallel service groups and switch over failover service groups on each of the nodes in the first half of the cluster:

  ```
  # hastop -local -evacuate
  ```

7 Unmount the VxFS file systems that are not managed by VCS.

- Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS mount point:
  
  ```
  # mount | grep vxfs
  # fuser -cu /mount_point
  ```

- Unmount the VxFS file system:
  
  ```
  # umount /mount_point
  ```

8 Verify that no VxVM volumes (other than VxVM boot volumes) remain open. Stop any open volumes that are not managed by VCS.

9 If you plan to upgrade the operating system, stop all ports.

  For 5.1x and 6.0 versions:
  
  ```
  # /optVRTS/install/installsfrc -stop node01 node02
  ```

### Step 2: Upgrading the first half of the cluster

Perform the following steps to upgrade the first half of the cluster.

#### To upgrade the first half of the cluster

1 If you plan to upgrade the operating system, rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:

  ```
  # mv /etc/llttab /etc/llttab.save
  ```

2 Upgrade the operating system, if required.
3 If you upgraded the operating system, restart the nodes:

```bash
# shutdown -r now
```

4 Rename the `/etc/llttab` file to its original name:

```bash
# mv /etc/llttab.save /etc/llttab
```

5 Make sure that you can run secure shell or remote shell from the node where you launched the installer to the nodes in the second subcluster without requests for a password.

6 On the first half of the cluster, upgrade SF Oracle RAC by using the `installmr` script. When you invoke the installer, select the **Full Upgrade** option. The installer automatically detects the phased upgrade though you select the Full Upgrade option.

```bash
# cd /tmp/sfha6.0.5
# ./installmr -base_path /tmp/sfha6.0.1 node01 node02
```

**Note:** Do not reboot the nodes in the first subcluster until you complete the instructions for preparing the second subcluster.

See “Step 3: Performing pre-upgrade tasks on the second half of the cluster” on page 80.

After you complete the upgrade of the first half of the cluster, no GAB ports will be shown in the output when you run the `gabconfig -a` command.

If you are upgrading from 5.0 releases that use regular license keys (not vxkeyless), then the installer shows the following warning. Select ‘n’ when prompted for additional liceses.

```
CPI WARNING V-9-40-5323 SFRAC license version 5.0 is not updated to 6.0 on node01. It’s recommended to upgrade to a 6.0 key.
CPI WARNING V-9-40-5323 SFRAC license version 5.0 is not updated to 6.0 on node02. It's recommended to upgrade to a 6.0 key.
```

SFRAC is licensed on the systems

Do you wish to enter additional licenses? [y,n,q,b] (n) n
Step 3: Performing pre-upgrade tasks on the second half of the cluster

Perform the following pre-upgrade steps on the second half of the cluster.

To perform the pre-upgrade tasks on the second half of the cluster

1. Stop all applications that are not configured under VCS but dependent on Oracle RAC or resources controlled by VCS. Use native application commands to stop the application.

   Note: The downtime starts now.

2. Stop all applications that are configured under VCS. Stop the Oracle database:
   - If the Oracle RAC instance is managed by VCS:
     ```bash
     # hagrp -offline oracle_group -sys node03
     # hagrp -offline oracle_group -sys node04
     ```
   - If the Oracle RAC instance is not managed by VCS, log in as the Oracle user on one of the nodes in the second half of the cluster and shut down the instances:
     For Oracle RAC 12c:
     ```bash
     $ srvctl stop instance -db db_name -node node_name
     ```
     For Oracle RAC 11.2.0.2 and later versions:
     ```bash
     $ srvctl stop instance -d db_name -n node_name
     ```
     For Oracle RAC 11.2.0.1 and earlier versions:
     ```bash
     $ srvctl stop instance -d db_name -i instance_name
     ```

3. Unmount the CFS file systems that are not managed by VCS.
   - Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:
     ```bash
     # mount | grep vxfs | grep cluster
     # fuser -cu /mount_point
     ```
4. Stop VCS on each of the nodes in the second half of the cluster:
   ```bash
   # hastop -local
   ```

5. Unmount the VxFs file systems that are not managed by VCS.
   ```bash
   # umount /mount_point
   ```

   Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFs or CFS mount point:
   ```bash
   # mount | grep vxfs
   # fuser -cu /mount_point
   ```

   Unmount the non-system VxFs file system:
   ```bash
   # umount /mount_point
   ```

6. Verify that no VxVM volumes (other than VxVM boot volumes) remain open.
   Stop any open volumes that are not managed by VCS.

7. Stop all ports.
   For 5.1x and 6.0 versions:
   ```bash
   # /opt/VRTS/install/installsfrc -stop node01 node02
   ```

Step 4: Performing post-upgrade tasks on the first half of the cluster

Perform the following post-upgrade steps on the first half of the cluster.
To perform the post-upgrade tasks on the first half of the cluster

1  On any one node on the first half of the cluster, force GAB to form a cluster.

   # /etc/init.d/llt start
   # /etc/init.d/gab start
   # gabconfig -x

2  On the first half of the cluster, start SF Oracle RAC:

   # cd /opt/VRTS/install
   # ./installsfrac<version> -start node1 node2

   Where <version> is the specific release version.

3  On the first half of the cluster, manually mount the VxFS or CFS file systems that are not managed by VCS.

4  Relink the SF Oracle RAC libraries with Oracle:

   Choose the option **Relink Oracle Database Binary** from the program menu.
5 Bring the Oracle database service group online.
   If the Oracle database is managed by VCS:
   
   # hagrp -online oracle_group -sys node_name
   
   If the Oracle database is not managed by VCS:
   
   For Oracle RAC 12c:
   
   $ srvctl start instance -db db_name \
   -node node_name
   
   For Oracle RAC 11.2.0.2 and later versions:
   
   $ srvctl start instance -d db_name \ 
   -n node_name
   
   For Oracle RAC 11.2.0.1 and earlier versions:
   
   $ srvctl start instance -d db_name \ 
   -i instance_name

   Note: The downtime ends here.

6 On the first half of the cluster, start all applications that are not managed by
   VCS. Use native application commands to start the applications.

Step 5: Upgrading the second half of the cluster
Perform the following steps to upgrade the second half of the cluster.

To upgrade the second half of the cluster

1 If you plan to upgrade the operating system, rename the /etc/llttab file to
   prevent LLT from starting automatically when the node starts:
   
   # mv /etc/llttab /etc/llttab.save

2 Upgrade the operating system, if required.
   For instructions, see the operating system documentation.

3 If you upgraded the operating system, restart the nodes:
   
   # shutdown -r now
4 Rename the `/etc/llttab` file to its original name:

```
# mv /etc/llttab.save /etc/llttab
```

5 Make sure that you can run secure shell or remote shell from the node where you launched the installer to the nodes in the second subcluster without requests for a password.

6 On the second half of the cluster, upgrade SF Oracle RAC with the `installmr` script.

When you invoke the installer, select the **Full Upgrade** option. The installer automatically detects the phased upgrade though you select the Full Upgrade option.

```
# cd /tmp/sfha6.0.5
# ./installmr -base_path /tmp/sfha6.0.1 node03 node04
```

If you are upgrading from 5.0 releases that use regular license keys (not `vxkeyless`), then the installer shows the following warning. Select 'n' when prompted for additional licenses.

CPI WARNING V-9-40-5323 SFRAC license version 5.0 is not updated to 6.0 on node01. It's recommended to upgrade to a 6.0 key.

CPI WARNING V-9-40-5323 SFRAC license version 5.0 is not updated to 6.0 on node02. It's recommended to upgrade to a 6.0 key.

SFRAC is licensed on the systems

Do you wish to enter additional licenses? [y,n,q,b] (n) n

---

**Step 6: Performing post-upgrade tasks on the second half of the cluster**

Perform the following post-upgrade steps on the second half of the cluster.

**To perform the post-upgrade tasks on the second half of the cluster**

1 Manually mount the VxFS and CFS file systems that are not managed by VCS.

2 On the second half of the cluster, start SF Oracle RAC:

```
# cd /opt/VRTS/install
# ./installsfra<version> -start node3 node4
```

Where `<version>` is the specific release version.
3 Relink the SF Oracle RAC libraries with Oracle:

If you want the installer to relink the Oracle Database Binary, you can choose the option **Relink Oracle Database Binary** from the menu.

Complete the remaining tasks to finish the upgrade.

4 Upgrade VxVM disk group version.

For instructions, see the chapter "Post-upgrade tasks" in the *Veritas Storage Foundation for Oracle RAC 6.0.1 Installation and Configuration Guide*.

5 Upgrade disk layout version.

For instructions, see the chapter "Post-upgrade tasks" in the *Veritas Storage Foundation for Oracle RAC 6.0.1 Installation and Configuration Guide*.

6 Bring the Oracle database service group online.

If the Oracle database is managed by VCS:

```bash
# hagrp -online oracle_group -sys node3
# hagrp -online oracle_group -sys node4
```

If the Oracle database is not managed by VCS:

For Oracle RAC 12c:

```bash
$ srvctl start instance -db db_name \
  -node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```bash
$ srvctl start instance -d db_name \
  -n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```bash
$ srvctl start instance -d db_name \
  -i instance_name
```

7 If the Oracle database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

```bash
# haconf -makerw
# hagrp -modify oracle_group AutoStart 1
# haconf -dump -makero
```
If the Oracle database is not managed by VCS, change the management policy for the database to automatic:

For Oracle RAC 12c:

```bash
$ srvctl modify database -db db_name -policy AUTOMATIC
```

For Oracle RAC 11g:

```bash
$ srvctl modify database -d db_name -y AUTOMATIC
```

8  Start all applications that are not managed by VCS. Use native application commands to start the applications.

9  Set or change the product license level, if required.

10 Migrate the SFDB repository database.

As root, dump out the old Sybase Adaptive Server Anywhere (Sybase ASA) repository. If you are using SFHA or SF Oracle RAC, you only need to do this on one node.

```bash
# /opt/VRTSdbed/migrate/sfua_rept_migrate
```

Performing an automated upgrade using response files with Install Bundles

Depending on the installed product, use one of the following procedures:

- Performing an automated upgrade of VCS, SFHA, or SFCFSHA using response files with Install Bundles
- Upgrading SF Oracle RAC using a response file

Performing an automated upgrade of VCS, SFHA, or SFCFSHA using response files with Install Bundles

Typically, you can use the response file that the installer generates after you perform VCS, SFHA, or SFCFSHA upgrade with Install Bundles on one system to upgrade VCS, SFHA, or SFCFSHA on other systems. You can also create a response file using the `makeresponsefile` option of the installer.
To perform automated VCS, SFHA, or SFCFSHA upgrade

1. Make sure the systems where you want to upgrade VCS, SFHA, or SFCFSHA meet the upgrade requirements.

2. Make sure the pre-upgrade tasks are completed.

3. Copy the response file to one of the systems where you want to upgrade SFHA.

4. Edit the values of the response file variables as necessary.

5. Mount the product disc and navigate to the folder that contains the installation program.

6. Start the upgrade from the system to the `/tmp/sfha6.1.1` directory. For example:

   ```
   # ./installmr -responsefile /tmp/response_file
   ```

   Where `/tmp/response_file` is the response file's full path name.

Upgrading SF Oracle RAC using a response file

Perform the steps in the following procedure to upgrade to 6.1.1 using a response file.

To upgrade SF Oracle RAC using a response file

1. Upgrade the operating system, if required.

   For instructions, see the operating system documentation.

2. Create a response file using one of the available options.

   **Note:** Make sure that you replace the host names in the response file with the names of the systems that you plan to upgrade.

   For more information, refer to *Veritas Storage Foundation for Oracle RAC 6.0.1 Installation and Configuration Guide*.

3. Navigate to the product directory on the installation media that contains the SF Oracle RAC installation program.
4 Start the installation:

```
# ./installmr -responsefile /tmp/response_file
```

Where `/tmp/response_file` is the full path name of the response file.

5 Complete the post-upgrade steps.

See the chapter "Performing post-upgrade tasks" in SF Oracle RAC 6.0.1 Installation Guide.

Performing rolling upgrade of SFHA Solutions using response files

Typically, you can use the response file that the installer generates after you perform SFHA Solutions upgrade on one system to upgrade SFHA Solutions on other systems.

You can also create a response file using the `makeresponsefile` option of the installer.

**To perform automated SFHA Solutions rolling upgrade**

1 Make sure the systems where you want to upgrade SFHA Solutions meet the upgrade requirements.

2 Make sure the pre-upgrade tasks are completed.

3 Copy the response file to the systems where you want to launch the installer.

   See the sample response file in the 6.1 Installation Guides.

4 Edit the values of the response file variables as necessary.

   See the response file variables in the 6.1 Installation Guides.

5 Mount the product disc and navigate to the folder that contains the installation program.

6 Start the upgrade from the system to which you copied the response file. For example:

   ```
   # ./installmr -responsefile /tmp/response_file
   ```

Performing a rolling upgrade using Install Bundles

You can use rolling upgrades to upgrade one product from a release to the next with minimal application downtime.

- Supported rolling upgrade paths
- Performing a rolling upgrade of VCS, SFHA, and SFCFSHA with Install Bundles
Performing a rolling upgrade of SF Oracle RAC with Install Bundles

Supported rolling upgrade paths

You can perform a rolling upgrade using the `installmr` script with Install Bundles. Table 3-7 shows the versions for which you can perform a rolling upgrade to 6.1.1.

Table 3-7: Supported rolling upgrade paths for Install Bundles

<table>
<thead>
<tr>
<th>Platform</th>
<th>version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>5.1, 5.1RPs</td>
</tr>
<tr>
<td></td>
<td>5.1SP1, 5.1SP1RPs</td>
</tr>
<tr>
<td></td>
<td>5.1SP1PR3, 6.0, 6.0RPs</td>
</tr>
<tr>
<td></td>
<td>6.0.1, 6.0.2, 6.0.3, 6.0.4, 6.0.5</td>
</tr>
</tbody>
</table>

**Note:** SLES11 doesn't support rolling upgrade to 6.1.1 from releases before 6.0.1.

**Note:** On RHEL6, SFHA Solutions only supports rolling upgrade to 6.1.1 from 5.1 SP1 RP4, 6.0.1, and 6.0.1 onwards.

**Note:** Before performing a rolling upgrade from version 5.1SP1RP3 to version 6.1.1, install patch VRTSvxfen-5.1SP1RP3P2. For downloading the patch, search VRTSvxfen-5.1SP1RP3P2 in Patch Lookup on the SORT website.

**OS upgrade support during rolling upgrades on Linux**

If the upgrade scenario involves operating system upgrades, SFHA Solutions supports rolling upgrade only for minor OS upgrades.

For the following scenarios, use phased upgrades instead of rolling upgrades:

- Upgrades from versions prior to 6.0.1 on SLES11 or SLES11 SP1 to 6.1.1 on SLES11 SP2.
- Upgrades from versions prior to 6.0.1 on RHEL6.1 or RHEL6.2 to 6.1.1 on RHEL6.
Performing a rolling upgrade of VCS, SFHA, and SFCFSHA with Install Bundles

Before you start the rolling upgrade, make sure that Symantec Cluster Server (VCS) is running.

To perform a rolling upgrade

1. Complete the preparatory steps on the first sub-cluster.
2. Log in as superuser.
3. Change to the /tmp/sfha6.1.1 directory.
4. Start the installer.
   
   # ./installmr -base_path /tmp/sfha6.1

5. From the menu, select Upgrade and from the sub menu, select Rolling Upgrade.
6. Enter one system of the cluster on which you would like to perform rolling upgrade.
7. The installer checks system communications, release compatibility, version information, and lists the cluster name, ID, and cluster nodes. Type y to continue.
8. The installer inventories the running service groups and determines the node or nodes to upgrade in phase 1 of the rolling upgrade. Type y to continue. If you choose to specify the nodes, type n and enter the names of the nodes.
9. The installer performs further prechecks on the nodes in the cluster and may present warnings. You can type y to continue or quit the installer and address the precheck's warnings.
10. Review the end-user license agreement, and type y if you agree to its terms.
11. After the installer shows the package list, it detects if there are online failover service groups on the nodes to be upgraded. If there are online failover service groups, the installer prompts you to do one of the following:
   - Manually switch service groups
   - Use the CPI to automatically switch service groups

   The downtime is the time that it normally takes for the service group's failover.
12 The installer prompts you to stop the applicable processes. Type y to continue.
   
The installer evacuates all service groups to the node or nodes that are not upgraded at this time. The installer stops parallel service groups on the nodes that are to be upgraded.

13 The installer stops relevant processes, uninstalls old kernel RPMs, and installs the new RPMs.
   
The installer performs the upgrade configuration and re-starts processes.
   
If some processes fail to start, you may need to reboot the nodes and manually check the cluster's status.

14 Complete the preparatory steps on the nodes that you have not yet upgraded.

15 The installer begins phase 1 of the upgrade on the remaining node or nodes. Type y to continue the rolling upgrade.
   
The installer repeats step 8 through step 13.
   
For clusters with larger number of nodes, this process may repeat several times. Service groups come down and are brought up to accommodate the upgrade.

16 When phase 1 of the rolling upgrade completes, begin phase 2 of the upgrade. Phase 2 of the upgrade includes downtime for the VCS engine (HAD), which does not include application downtime. Type y to continue.

17 The installer determines the remaining RPMs to upgrade. Press Enter to continue.

18 The installer stops Symantec Cluster Server (VCS) processes but the applications continue to run. Type y to continue.
   
The installer performs prechecks, uninstalls old RPMs, and installs the new RPMs. It performs post-installation tasks, and the configuration for the upgrade.

19 A prompt message appears to ask if you would like to send the information about this installation to Symantec to help improve installation in the future? Type y or n to help Symantec improve the installation.

20 If you have network connection to the Internet, the installer checks for updates. If updates are discovered, you can apply them now.
A prompt message appears to ask if the user would like to read the summary file. You can choose y if you want to read the install summary file.

If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.

Performing a rolling upgrade of SF Oracle RAC with Install Bundles

Use a rolling upgrade to upgrade Symantec Storage Foundation for Oracle RAC to the latest release with minimal application downtime.

Using the installmr script with Install Bundles, you can upgrade to 6.1.1 from releases earlier than 6.1.

- Preparing to perform a rolling upgrade to SF Oracle RAC 6.1.1
- Using Install Bundles to perform a rolling upgrade of SF Oracle RAC

Preparing to perform a rolling upgrade to SF Oracle RAC 6.1.1

Perform the preparatory steps in this section if you are performing a rolling upgrade of the cluster. Before you upgrade, make sure that your systems meet the hardware and software requirements for this release.

To prepare to upgrade SF Oracle RAC

Perform the steps on the first subcluster.
1. Log in as superuser to one of the nodes in the subcluster.

2. Back up the following configuration files on your system:
   - main.cf, types.cf, CVMTypes.cf, CFSTypes.cf, OracleTypes.cf, OracleASMTypes.cf,
   - PrivNIC.cf, MultiPrivNIC.cf, CRSResource.cf, /etc/llttab, /etc/llthosts, /etc/gabtab, /etc/vxfentab, /etc/vxfendg, /etc/vxfenmode

   For example:
   ```bash
   # cp /etc/VRTSvcs/conf/config/main.cf \
   /etc/VRTSvcs/conf/config/main.cf.save
   ```

3. Installer verifies that recent backups of configuration files in VxVM private region have been saved in /etc/vx/cbr/bk.
   If not, a warning message will be displayed after `installmr upgrade prechecks`.

   **Warning:** Backup `/etc/vx/cbr/bk` directory.

4. Stop the Oracle RAC resources on each node.
   - If the database instances are managed by VCS, take the corresponding VCS service groups offline. As superuser, enter:
     ```bash
     # hagrp -offline oracle_group -sys node_name
     ```
   - If the database instances are not managed by VCS, then run the following on one node:
     For Oracle RAC 12c:
     ```bash
     # srvctl stop instance -db db_name -node node_name
     ```
     For Oracle RAC 11.2.0.2 and later versions:
     ```bash
     $ srvctl stop instance -d db_name \
     -n node_name
     ```
     For Oracle RAC 11.2.0.1 and earlier versions:
     ```bash
     $ srvctl stop instance -d db_name \
     -i instance_name
     ```

5. If the Oracle database is managed by VCS, set the AutoStart value to 0 to prevent the database service group from starting automatically when VCS starts. Failing to perform this step results in the database attempting to
come online after the upgrade; the attempt fails due to the presence of old libraries on the system.

```bash
# haconf -makerw
# hagrp -modify oracle_group AutoStart 0
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to manual:
  - For Oracle RAC 12c:
    ```bash
    $ srvctl modify database -db db_name -policy MANUAL
    ```
  - For Oracle RAC 11g:
    ```bash
    $ srvctl modify database -d db_name -y MANUAL
    ```

6. Unmount all the CFS file system which is not under VCS control.

```bash
# mount |grep vxfs | grep cluster
# fuser -m /mount_point
# umount /mount_point
```

Make sure that no processes are running which make use of mounted shared file system or shared volumes.

```bash
# fuser -cu /mount_point
```

7. Take all the parallel VCS service groups offline on each of the nodes in the current subcluster:

```bash
# hagrp -offline grp_name -sys sys_name
```
8 Unmount all the VxFS file system which is not under VCS control.

# mount |grep vxfs
# fuser -m /mount_point
# umount /mount_point

9 If you plan to continue using the Storage Foundation for Databases (SFDB) tools, you must prepare to migrate the SFDB repository database before upgrading to SF Oracle RAC 6.1.1.

See “Pre-upgrade tasks for migrating the SFDB repository database” on page 35.

Using Install Bundles to perform a rolling upgrade of SF Oracle RAC

Before you start the rolling upgrade, make sure that Symantec Cluster Server (VCS) is running.

To perform a rolling upgrade

1 If you want to upgrade the operating system, perform the following steps:

Note: If you plan to upgrade the operating system, make sure that you upgrade all nodes before you start rolling upgrade of SF Oracle RAC.

- Change to the /opt/VRTS/install directory on the node where you want to upgrade the operating system:

  # cd /opt/VRTS/install

- Stop SF Oracle RAC:

  # ./installsfrac<version> -stop

  Where <version> is the specific release version.

- Upgrade the operating system. For instructions, see the operating system documentation.

- Reboot the nodes:
# shutdown -r now

2 Complete the preparatory steps on the first sub-cluster.

See "Preparing to perform a rolling upgrade to SF Oracle RAC 6.1.1" on page 92.

3 Log in as superuser.

4 Change to the sfha6.1.1 directory.

5 Start the installmr script.

```bash
# . /installmr -base_path /tmp/sfha6.1/
```

6 From the menu, select Upgrade and from the sub menu, select Rolling Upgrade.

7 The installer suggests system names for the upgrade. Enter Yes to upgrade the suggested systems, or enter No, and then enter the name of any one system in the cluster on which you want to perform a rolling upgrade.

8 The installer checks system communications, release compatibility, version information, and lists the cluster name, ID, and cluster nodes. Type y to continue.

9 The installer inventories the running service groups and determines the node or nodes to upgrade in phase 1 of the rolling upgrade. Type y to continue. If you choose to specify the nodes, type n and enter the names of the nodes.

See "Pre-upgrade tasks for migrating the SFDB repository database" on page 35.

10 The installer performs further prechecks on the nodes in the cluster and may present warnings. You can type y to continue or quit the installer and address the precheck's warnings.

11 Review the end-user license agreement, and type y if you agree to its terms.

12 The installer lists the RPMs to upgrade on the selected node or nodes.

13 After the installer shows the package list, it detects if there are online failover service groups on the nodes to be upgraded. If there are online failover service groups, the installer prompts you to do one of the following:

   - Manually switch service groups
   - Use the CPI to automatically switch service groups

The downtime is the time that it normally takes for the service group's failover.
14 The installer prompts you to stop the applicable processes. Type y to continue.
The installer evacuates all service groups to the node or nodes that are not
upgraded at this time. The installer stops parallel service groups on the nodes
that are to be upgraded.

15 The installer stops relevant processes, uninstalls old kernel RPMs, and installs
the new RPMs.
The installer performs the upgrade configuration and re-starts processes.
If some processes fail to start, you may need to reboot the nodes and manually
check the cluster's status.

Note: The Oracle service group is offline as the AutoStart attribute is set to 0
to prevent the service group from starting automatically. The service group is
started later in the process.

16 Manually mount the VxFS and CFS file systems that are not managed by VCS.

17 Relink the SF Oracle RAC libraries with Oracle:
Choose the option **Relink Oracle Database Binary** from the program menu.

18 Bring the Oracle database service group online.
   - If VCS manages the Oracle database:
     
     ```bash
     # hagrp -online oracle_group -sys node_name
     ```
   - If VCS does not manage the Oracle database:
     For Oracle RAC 11g:
     ```bash
     $ srvctl start database -d db_name
     ```
     For Oracle RAC 12c:
     ```bash
     $ srvctl start database -db db_name
     ```

19 Start all applications that are not managed by VCS. Use native application
commands to start the applications.

20 Complete the preparatory steps on the nodes that you have not yet upgraded.
21 If the nodes are rebooted, restart the installer and continue phase-1 for second sub-cluster. Type y to continue the rolling upgrade.

The installer repeats step 7 through step 17.

For clusters with larger number of nodes, this process may repeat several times. Service groups come down and are brought up to accommodate the upgrade.

This completes phase 1 of the upgrade.

22 ■ If VCS manages the Oracle database, reset the AutoStart value to 1 to enable VCS to bring the database service group online when VCS starts:

```
# haconf -makerw
# hagrp -modify oracle_group AutoStart 1
# haconf -dump -makero
```

■ If VCS does not manage the Oracle database, change the management policy for the database to automatic:

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y AUTOMATIC
```

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy AUTOMATIC
```

23 If the Sybase database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the service group online when VCS starts:

```
# haconf -makerw
# hagrp -modify sybasece AutoStart 1
# haconf -dump -makero
```

24 Migrate the SFDB repository database.

As root, dump out the old Sybase Adaptive Server Anywhere (Sybase ASA) repository. If you are using SFHA or SF Oracle RAC, you only need to do this on one node.

```
# /opt/VRTSdbed/migrate/sfua_rept_migrate
```

25 When phase 1 of the rolling upgrade completes, begin phase 2 of the upgrade. Phase 2 of the upgrade includes downtime for the VCS engine (HAD), which does not include application downtime. Type y to continue.
26 Phase 2 of the upgrade begins here. This phase includes downtime for the VCS engine (HAD), which does not include application downtime. Type y to continue.

27 The installer determines the remaining RPMs to upgrade. Press Enter to continue.

28 The installer stops Symantec Cluster Server (VCS) processes but the applications continue to run. Type y to continue.

The installer performs prechecks, uninstalls old RPMs, and installs the new RPMs. It performs post-installation tasks, and the configuration for the upgrade.

29 When the following message appears, type y or n to help Symantec improve the installation:

Would you like to send the information about this installation to Symantec to help improve installation in the future?

30 If you have network connection to the Internet, the installer checks for updates. If updates are discovered, you can apply them now.

31 A prompt message appears to ask if the user would like to read the summary file. You can choose y if you want to read the install summary file.

32 If you want to upgrade the application clusters that use CP server based fencing to version 6.1 and later, make sure that you first upgrade VCS or SFHA on the CP server systems to version 6.1 and later. And then, upgrade all application clusters. The CP server with version 6.1 and later supports application clusters on 6.1 and later (HTTPS-based communication) and application clusters before 6.1 (IPM-based communication). When you configure the CP server, the installer asks the VIPs for HTTPS-based communication (to support clients on release version 6.1 and later) and VIPs for IPM-based communication (to support clients on release versions before 6.1).

For instructions to upgrade VCS or SFHA on the CP server systems, refer to the appropriate installation guide.
Upgrading to 6.1.1 from 6.1

This chapter includes the following topics:

- About using the installer to upgrade from 6.1 when the root disk is encapsulated
- Prerequisites for upgrading to 6.1.1
- Downloading required software to upgrade to 6.1.1
- Performing a full upgrade to 6.1.1 on a cluster
- Upgrading to 6.1.1 on a standalone system
- Performing a phased upgrade to SFCFSHA and SFRAC
- Upgrading to 6.1.1 on a system that has encapsulated boot disk
- Performing a rolling upgrade using the installer
- Upgrading the operating system
- Upgrading SFHA with the Veritas Web-based installer
- Verifying software versions

About using the installer to upgrade from 6.1 when the root disk is encapsulated

When you use the installer to upgrade from a previous version of SFHA Solutions and the system where you plan to upgrade has an encapsulated root disk, you may have to unencapsulate it.
Prerequisites for upgrading to 6.1.1

If you are upgrading from 6.1, see the following list for prerequisites for upgrading to the 6.1.1 release:

- For any product in the Symantec Storage Foundation stack, you must have the 6.1.1 release binaries.
- Each system must have sufficient free space to accommodate patches.
- The full list of prerequisites can be obtained by running ./installmr -precheck.
- Make sure to download the latest patches for the installer.
  See “Downloading required software to upgrade to 6.1.1 ” on page 101.

For information on supported upgrade types, See “Supported upgrade types" on page 18.

Table 4-1 Upgrading using the installer from 6.1 when the root disk is encapsulated

<table>
<thead>
<tr>
<th>Starting version</th>
<th>Ending version</th>
<th>Action required</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>6.1.1</td>
<td>Do not unencapsulate. The installer runs normally. Reboot after upgrade.</td>
</tr>
</tbody>
</table>

Performing a full upgrade to 6.1.1 on a cluster

Performing a full upgrade on a cluster requires stopping cluster failover functionality during the entire procedure.

Depending on your cluster's configuration, select one of the following procedures to upgrade to 6.1.1:

- Performing a full upgrade to 6.1.1 on a Symantec Cluster Server
- Performing a full upgrade to 6.1.1 on an SFHA cluster

Downloading required software to upgrade to 6.1.1

This section describes how to download the latest patches for the installer.

To download required software to upgrade to 6.1.1

2. Extract it to a directory, say /tmp/sfha611.
Performing a full upgrade to 6.1.1 on an SFHA cluster

Performing a full upgrade to 6.1.1 on an SF Oracle RAC cluster

Performing a full upgrade to 6.1.1 on a Symantec Cluster Server

The following procedure describes performing a full upgrade on a Symantec Cluster Server (VCS) cluster.

---

**Note:** You need to make sure that IPv4RouteOptions attribute is configured for MultiNICA resources, otherwise network connection may be interrupted.

---

**To upgrade VCS**

1. Make sure you have downloaded the latest software required for the upgrade.
   
   See "Downloading required software to upgrade to 6.1.1" on page 101.
   
2. Log in as superuser.

   **Note:** Upgrade the Operating System and reboot the systems if required.

3. Check the readiness of the nodes where you plan to upgrade. From the directory that contains the extracted and untarred 6.1.1 rolling patch binaries, change to the directory that contains the installmr script. Start the pre-upgrade check:

   ```
   # ./installmr -precheck node01 node02 ... nodeN
   ```

4. Resolve any issues that the precheck finds.

5. Start the upgrade:

   ```
   # ./installmr node01 node02 ... nodeN
   ```

6. After the upgrade, review the log files for any issues.

---

Performing a full upgrade to 6.1.1 on an SFHA cluster

The following procedure describes performing a full upgrade on an SFHA and VCS cluster.

**To perform a full upgrade to 6.1.1 on an SFHA cluster**

1. Make sure you have downloaded the latest software required for the upgrade.
Performing a full upgrade to 6.1.1 on an SFCFSHA cluster

To perform a full upgrade to 6.1.1 on an SFCFSHA cluster

1 Make sure you have downloaded the latest software required for the upgrade. See “Downloading required software to upgrade to 6.1.1” on page 101.

2 Log in as superuser.

3 If applications are not managed by VCS, make the applications offline.

4 On each node, enter the following command to check if any Storage Checkpoints or VxFS file systems out of VCS control are mounted:

   # mount | grep vxfs

   If any Storage Checkpoints or VxFS file systems are mounted, on each node in the cluster umount all Storage Checkpoints.

   # umount /checkpoint_name

Performing a full upgrade to 6.1.1 on a cluster

- Log in as superuser.
- From the directory that contains the extracted and untarred 6.1.1 rolling patch binaries, change to the directory that contains the installmr script. Check the readiness of the nodes where you plan to upgrade. Start the pre-upgrade check:

  # ./installmr -precheck node01 node02... nodeN

  where node01, node02 and nodeN are nodes to be upgraded.

- If service groups have VxFS file systems mounted, make the service groups offline.

- If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the installmr script:

  # sfcache offline cache_area

- Start the upgrade:

  # ./installmr node01 node02... nodeN

  where node01, node02 and nodeN are nodes to be upgraded.
5 If you have created any Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:
   - Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
   - Use the vxrvg stop command to stop each RVG individually:
     
     ```
     # vxrvg -g diskgroup stop rvg_name
     ```
   - On the Primary node, use the vxrlink status command to verify that all RLINKs are up-to-date:
     
     ```
     # vxrlink -g diskgroup status rlink_name
     ```

   Caution: To avoid data corruption, do not proceed until all RLINKs are up-to-date.

6 If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the installmr script:

   ```
   # sfcache offline cache_area
   ```

7 Stop activity to all VxVM volumes.
   For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes

8 Stop all VxVM volumes by entering the following command for each disk group on master node:

   ```
   # vxvol -g diskgroup stopall
   ```

   Verify that no volumes remain open:

   ```
   # vxprint -Aht -e v_open
   ```

9 On each node, stop the VCS command server:

   ```
   # ps -ef | grep CmdServer
   # kill -9 pid_of_CmdServer
   ```

   `pid_of_CmdServer` is the process ID of CmdServer.

10 If required, apply the OS kernel patches.
From the directory that contains the extracted and untarred 6.1.1 rolling patch binaries, change to the directory that contains the installmr script. Start the upgrade.

```
# ./installmr node01 node02
```

where `node01` and `node02` are nodes which are to be upgraded.

After all nodes in the cluster are upgraded, the processes will be restarted automatically. Should there be any problem, the `installmr` script will ask you to reboot the system. Then the application failover capability will be available.

If necessary, reinstate any missing mount points in the `/etc/filesystems` file on each node.

Restart all the volumes by entering the following command on the master node, for each disk group:

```
# vxvol -g diskgroup startall
```

If you stopped any RVGs in step 5, restart each RVG:

```
# vxrvg -g diskgroup start rvg_name
```

Remount all VxFS file systems and Storage Checkpoints on all nodes:

```
# mount /filesystem
```

Performing a full upgrade to 6.1.1 on an SF Oracle RAC cluster

The following procedure describes performing a full upgrade on an SF for Oracle RAC cluster.

To upgrade to 6.1.1 on an SF Oracle RAC cluster

1. Make sure you have downloaded the latest software required for the upgrade.
2. Log in as superuser.
3. Verify that `/opt/VRTSvcs/bin` is in your `PATH` so that you can execute all product commands.
4. From any node in the cluster, make the VCS configuration writable:

```
# haconf -makerw
```
5 Enter the following command to freeze HA service group operations on each node:

```bash
# hasys -freeze -persistent nodename
```

6 Make the configuration read-only:

```bash
# haconf -dump -makero
```

7 If the Oracle database is managed by VCS, set the AutoStart value to 0 to prevent the database service group from starting automatically when VCS starts:

```bash
# haconf -makerw
# hagrp -modify oracle_group AutoStart 0
# haconf -dump -makero
```

- If the Oracle database is not managed by VCS, change the management policy for the database to manual:
  For Oracle RAC 12c:

```bash
$ srvctl modify database -db db_name -policy MANUAL
```

  For Oracle RAC 11g:

```bash
$ srvctl modify database -d db_name -y MANUAL
```

8 If Oracle Clusterware is not controlled by VCS, enter the following command on each node of the cluster to stop Oracle Clusterware:

```bash
# GRID_HOME/bin/crsctl stop crs
```

9 Stop all applications that use VxFS or VxVM disk groups, whether local or CFS. If the applications are under VCS control:

```bash
# hagrp -offline grp_name -any
```

If the applications are not under VCS control:

Use native application commands to stop the application.
10 Unmount the VxFS file system, which is not under VCS control.

    # mount |grep vxfs
    # fuser -m /mount_point
    # umount /mount_point

Make sure that no processes are running which make use of mounted shared
file system or shared volumes.

    # fuser -cu /mount_point

11 If you have VxVM or VxFS cache on your system, offline the cache before
upgrading with the `installmr` script:

    # sfcache offline cache_area

12 Stop VCS.

    # hastop -all

13 If required, apply the OS kernel patches.

    See Oracle’s documentation for the procedures.

14 From the directory that contains the extracted and untarred 6.1.1 rolling patch
binaries, change to the directory that contains the installmr script. Enter:

    # ./installmr node01 node02

where `node01` and `node02` are nodes which are to be upgraded.

15 Follow the instructions from the installer. If there is some module load/unload
issue, reboot all of the nodes of the cluster.

    # /sbin/shutdown -r now

16 If necessary, reinstate any missing mount points in the `/etc/fstab` file on each
node.

17 Relink the SF Oracle RAC libraries with Oracle:

    Choose the option **Relink Oracle Database Binary** from the program menu.

18 From any node in the cluster, make the VCS configuration writable:

    # haconf -makerw
19 Enter the following command on each node to unfreeze HA service group operations:

```
# hasys -unfreeze -persistent nodename
```

20 Make the configuration read-only:

```
# haconf -dump -makero
```

21 Enter the following command on each node to take service groups online:

```
# hagrp -online service_group -sys nodename
```

22 Restart all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup startall
```

23 Remount all VxFS file systems on all nodes:

```
# mount /filesystem
```

24 If Oracle Clusterware is not controlled by VCS, enter the following command on each node to start Oracle Clusterware.

```
# $CRS_HOME/bin/crsctl start crs
```

25 Bring the Oracle database service group online.

- If the Oracle database is managed by VCS:

```
# hagrp -online Oracle_group -any
```

- If the Oracle database is not managed by VCS:

  For Oracle RAC 11g:

  
  ```
  $ srvctl start database -d db_name
  ```

  For Oracle RAC 12c:

  ```
  $ srvctl start database -db db_name
  ```

26 If the Oracle database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:
# haconf -makerw
# hagrp -modify oracle_groupname AutoStart 1
# haconf -dump -makero

- If the Oracle database is not managed by VCS, change the management policy for the database to automatic:
  For Oracle RAC 11g:
  
  ```
  $ srvctl modify database -d db_name -y AUTOMATIC
  ```
  
  For Oracle RAC 12c:
  
  ```
  $ srvctl modify database -db db_name -policy AUTOMATIC
  ```

27 Upgrade Oracle RAC.

For information on Oracle RAC support, see:

http://www.symantec.com/docs/DOC5081

For instructions, see the chapter Upgrading Oracle RAC in Symantec™ Storage Foundation for Oracle® RAC Installation and Configuration Guide.

Note: The procedure for Oracle RAC 12c is the same with that for Oracle RAC 11g Release 2.

---

**Upgrading to 6.1.1 on a standalone system**

You can use this procedure to upgrade on a standalone system that runs SF.

**To upgrade to 6.1.1 on a standalone system**

1 Make sure you have downloaded the latest software required for the upgrade.

2 Log in as superuser.

3 Verify that `/opt/VRTS/bin` is in your `PATH` so you can execute all product commands.

4 If required, apply the OS kernel patches.

5 Enter the following command to check if any VxFS file systems or Storage Checkpoints are mounted:

  ```
  # df -T | grep vxfs
  ```
6 Unmount all Storage Checkpoints and file systems:

```
# umount /checkpoint_name
# umount /filesystem
```

7 If you have created any Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

- Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
- Use the `vxrvg stop` command to stop each RVG individually:

  ```
  # vxrvg -g diskgroup stop rvg_name
  ```

- On the Primary node, use the `vxrlink status` command to verify that all RLINKs are up-to-date:

  ```
  # vxrlink -g diskgroup status rlink_name
  ```

  **Caution:** To avoid data corruption, do not proceed until all RLINKs are up-to-date.

8 If you have VxVM or VxFScache on your system, offline the cache before upgrading with the `installmr` script:

```
# sfcache offline cache_area
```

9 Stop activity to all VxVM volumes. For example, stop any applications such as databases that access the volumes, and unmount any file systems that have been created on the volumes.

10 Stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open:

```
# vxprint -Aht -e v_open
```

11 Navigate to the folder that contains the installation program. Run the `installmr` script:

```
# ./installmr nodename
```
12 If necessary, reinstate any missing mount points in the `/etc/fstab` file.

13 Restart all the volumes by entering the following command for each disk group:

```
# vxvol -g diskgroup startall
```

14 If you stopped any RVGs in step 7, restart each RVG:

```
# vxrvg -g diskgroup start rvg_name
```

15 Remount all VxFS file systems and Storage Checkpoints:

```
# mount /filesystem
# mount /checkpoint_name
```

Performing a phased upgrade to SFCFSHA and SFRAC

This section describes how to perform a phased upgrade to SFCFSHA and SFRAC.

Performing a phased upgrade of SFCFSHA

Performing a phased upgrade involves the following tasks:

- Preparing the first subcluster
- Upgrading the SFCFSHA stack on the first subcluster
- Preparing the second subcluster
- Activating the first subcluster
- Upgrading the operating system on the second subcluster
- Upgrading the second subcluster
- Finishing the phased upgrade

Before you start the upgrade on the first half of the cluster, back up the VCS configuration files `main.cf` and `types.cf` which are in the directory `/etc/VRTSvcs/conf/config/`.

Prerequisites for a phased upgrade

Before you start the upgrade, confirm that you have licenses for all the nodes that you plan to upgrade. Note that your applications have downtime during this procedure.
Planning for a phased upgrade

Plan out the movement of the service groups from node-to-node to minimize the downtime for any particular service group. Some basic guidelines follow:

- Split the cluster in half. If the cluster has an odd number of nodes, calculate \((n+1)/2\), and start the upgrade with the even number of nodes.
- Split the cluster so that your high priority service groups remain online during the upgrade of the first subcluster.

Phased upgrade limitations

The following limitations primarily describe not to tamper with configurations or service groups during the phased upgrade:

- While you perform the upgrades, do not start any modules. Also, do not add or remove service groups to any of the nodes.
- Depending on your configuration, you may find that you cannot upgrade multiple nodes at the same time. You may only be able to upgrade one node at a time.
- For very large clusters, you might have to repeat these steps multiple times to upgrade your cluster.
- You can perform a phased upgrade when the root disk is encapsulated.

Preparing the first subcluster

To move the service groups to the second subcluster

1. Switch failover groups from the first half of the cluster to one of the nodes in the second half of the cluster. In this procedure, node01 is a node in the first half of the cluster and node04 is a node in the second half of the cluster. Enter the following:

   ```
   # hagrp -switch failover_group -to node04
   ```

2. On the first half of the cluster, stop all applications that are not configured under VCS. Use native application commands to stop the applications.
On the first half of the cluster, unmount the VxFS or CFS file systems that are not managed by VCS.

```bash
# mount | grep vxfs
```

Verify that no processes use the VxFS or CFS mount point. Enter the following:

```bash
# fuser -c /mount_point
```

Stop any processes using a VxFS or CFS mount point with the mechanism provided by the application.

Unmount the VxFS or CFS file system. Enter the following:

```bash
# umount /mount_point
```

On the first half of the cluster, bring all the VCS service groups offline including CVM group. Enter the following:

```bash
# hagrp -offline group_name -sys node01 node02
```

When the CVM group becomes OFFLINE, all the parallel service groups such as the CFS file system will also become OFFLINE on the first half of the cluster nodes.

Verify that the VCS service groups are offline on all the nodes in first half of the cluster. Enter the following:

```bash
# hagrp -state group_name
```

If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the `installmr` script:

```bash
# sfcache offline cache_area
```

Freeze the nodes in the first half of the cluster. Enter the following:

```bash
# haconf -makerw
# hasys -freeze -persistent node01
# haconf -dump -makero
```
If I/O fencing is enabled, then on each node of the first half of the cluster, change the contents of the `/etc/vxfenmode` file to configure I/O fencing in disabled mode.

If you are in the CPS fencing mode, Symantec recommends you making a backup of the `/etc/vxfenmode` file for future use:

```
# cp /etc/vxfenmode /etc/vxfenmode.bak
```

To change the contents of the `/etc/vxfenmode` file to configure I/O fencing in disabled mode, enter the following:

```
# cp /etc/vxfen.d/vxfenmode_disabled /etc/vxfenmode
# cat /etc/vxfenmode
[root@swlx08 ~]# cat /etc/vxfenmode
#
# vxfen_mode determines in what mode VCS I/O Fencing should work.
#
# available options:
# scsi3 - use scsi3 persistent reservation disks
# customized - use script based customized fencing
# disabled - run the driver but don't do any actual fencing
#
# vxfen_mode=disabled
```

If the cluster-wide attribute UseFence is set to SCSI3, then reset the value to NONE in the `/etc/VRTSvcs/conf/config/main.cf` file, in first half of the cluster.

Verify that only GAB ports a, b, d and h are open. Enter the following:

```
# gabconfig -a
GAB Port Memberships
====================================================================
Port a gen 6b5901 membership 01
Port b gen 6b5904 membership 01
Port d gen 6b5907 membership 01
Port h gen ada40f membership 01

Do not stop VCS. Port h should be up and running.
```
11 In the first half of the cluster, stop all VxVM and CVM volumes. Enter the following command for each disk group:

```
# vxvol -g diskgroup stopall
```

Verify that no volumes remain open. Enter the following:

```
# vxprint -Aht -e v_open
```

12 On first half of the cluster, upgrade the operating system on all the nodes, if applicable. For instructions, see the upgrade paths for the operating system.

**Upgrading the SFCFSHA stack on the first subcluster**

To upgrade the SFCFSHA stack on the first subcluster

- **Note:** This procedure is based on an "in-place" upgrade path; that is, if the minor operating system is upgraded, the release will be the same, but only the path level will change. If you are moving from major operating system release to another, you must uninstall the SFCFSHA stack before you upgrade the operating system. After the operating system is upgraded, you must reinstall SFCFSHA.

On the first half of the cluster, upgrade SFCFSHA by using the installmr script. For example use the installmr script as shown below:

```
# ./installmr node01 node02
```

where `<node01>` and `<node02>` are the nodes on the first subcluster.

After the upgrade for first half of the cluster is complete, no GAB ports will be shown in `gabconfig -a` output.

To upgrade your operating system, follow the normal procedures for your platform.

- **Note:** After the installation completes, you can safely ignore any instructions that the installer displays.
Preparing the second subcluster

To prepare the second subcluster

1. On the second half of the cluster, stop all applications that are not configured under VCS. Use native application commands to stop the application. [Downtime starts now.]

2. On the second half of the cluster, unmount the VxFS and CFS file systems that are not managed by VCS. Enter the following:

   # mount | grep vxfs

   Verify that no processes use the VxFS and CFS mount point. Enter the following:

   # fuser -c /mount_point

   Stop any processes using a VxFS and CFS mount point with the mechanism provided by the application.

   Unmount the VxFS and CFS file system. Enter the following:

   # umount /mount_point

3. On the second half of the cluster, unfreeze all the VCS service groups on all the nodes using the following commands:

   # haconf -makerw
   # hagrp -unfreeze group_name -persistent
   # haconf -dump -makero

4. On the second half of the cluster, bring all the VCS service groups offline, including CVM group. Enter the following:

   # hagrp -offline group_name -sys node03 node04

5. On the second half of the cluster, verify that the VCS service groups are offline. Enter the following:

   # hagrp -state group_name

6. If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the installmr script:

   # sfcache offline cache_area
7 Stop VCS on the second half of the cluster. Enter the following:

    # hastop -local

8 On each node of the second half of the cluster, change the contents of the
/etc/vxfenmode file to configure I/O fencing in disabled mode.

    # cp /etc/vxfen.d/vxfenmode_disabled /etc/vxfenmode
    # cat /etc/vxfenmode
    # vxfen_mode determines in what mode VCS I/O Fencing should work.
    #
    # available options:
    # scsi3 - use scsi3 persistent reservation disks
    # customized - use script based customized fencing
    # disabled - run the driver but don't do any actual fencing
    #
    vxfen_mode=disabled

9 If the cluster-wide attribute UseFence is set to SCSI3, reset the value to NONE
in the /etcVRTSvcs/conf/config/main.cf file, in second half of the cluster.

10 On the second half on cluster, stop the following SFCFSHA modules: VCS,
VxFEN, ODM, GAB, and LLT. Enter the following:

    # /etc/init.d/vxglm stop
    # /etc/init.d/vxodm stop
    # /etc/init.d/vxgms stop
    # /etc/init.d/vxfen stop
    # /etc/init.d/gab stop
    # /etc/init.d/llt stop
11 On each node in the first half of the cluster, enable fencing. Replace the /etc/vxfemode file with your previous vxfenmode file. Take the scsi3_dmp file as an example:

```
# cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
# cat /etc/vxfenmode
#
# vxfen_mode determines in what mode VCS I/O Fencing should work.
#
# available options:
# scsi3    - use scsi3 persistent reservation disks
# customized - use script based customized fencing
# sybase   - use scsi3 disks in kernel but coordinate membership
# with Sybase ASE
# disabled - run the driver but don't do any actual fencing
#
# vxfen_mode=scsi3
#
# scsi3_disk_policy determines the way in which I/O Fencing
# communicates with the coordination disks.
#
# available options:
# dmp      - use dynamic multipathing
# raw      - connect to disks using the native interface
#
# scsi3_disk_policy=dmp
```

12 If the cluster-wide attribute UseFence is set to NONE, reset the value to SCSI3 in the /etc/VRTSvcs/conf/config/main.cf file, in first half of the cluster.

**Activating the first subcluster**

To activate the first subcluster

1 Run the installer to start SFCFSHA:

```
# /opt/VRTS/install/installsfcfsha611 -start node01 node02
```

2 Start LLT and GAB on the first subcluster:

```
# /etc/init.d/llt start
# /etc/init.d/gab start
```
3  Force gab to form a cluster in the first half of the cluster.
   # /sbin/gabconfig -x
   GAB port a appears in gabconfig -a command output.

4  On the first half of the cluster, bring the VCS service groups online. Enter the following:
   # hagrp -online group_name -sys node_name
   After you bring the CVM service group ONLINE, all the GAB ports u, v, w and f come ONLINE and all the CFS mounts service groups also come ONLINE automatically.

5  Manually mount the VxFS and CFS file systems that are not managed by VCS.
   [Downtime ends now.]

Upgrading the operating system on the second subcluster
You can perform the operating system upgrade on the second subcluster, if required.
Before performing operating system upgrade, it is better to prevent LLT from starting automatically when the node starts. For example, you can do the following:
   # mv /etc/llttab /etc/llttab.save
   or you can change the /etc/default/llt file by setting LLT_START = 0.
   After you finish upgrading the OS, remember to change the LLT configuration to its original configuration.
   Refer to the operating system's documentation for more information.

Upgrading the second subcluster
To upgrade the second subcluster
   ◆  Enter the following:
      # ./installmr node03 node04
Completing the phased upgrade

To complete the phased upgrade

1. Verify that the cluster UUID on the nodes in the second subcluster is the same as the cluster UUID on the nodes in the first subcluster. Run the following command to display the cluster UUID:

   ```
   # /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus -display nodename
   ```

   If the cluster UUID differs, manually copy the cluster UUID from a node in the first subcluster to the nodes in the second subcluster. For example:

   ```
   # /opt/VRTSvcs/bin/uuidconfig.pl [-rsh] -clus -copy -from_sys node01 -to_sys node03 node04
   ```

2. On each node in the second half of the cluster, enable fencing. Enter the following:

   ```
   # cp /etc/vxfen.d/vxfenmode_scsi3_dmp /etc/vxfenmode
   # cat /etc/vxfenmode
   #
   # vxfen_mode determines in what mode VCS I/O Fencing should work.
   #
   # available options:
   # scsi3 - use scsi3 persistent reservation disks
   # customized - use script based customized fencing
   # sybase - use scsi3 disks in kernel but coordinate
   # membership with Sybase ASE
   # disabled - run the driver but don't do any actual fencing
   #
   vxfen_mode=scsi3
   #
   # scsi3_disk_policy determines the way in which I/O Fencing
   # communicates with the coordination disks.
   #
   # available options:
   # dmp - use dynamic multipathing
   # raw - connect to disks using the native interface
   #
   scsi3_disk_policy=dmp
   ```

3. Start SFCFSHA using the installer:

   ```
   # /opt/VRTS/install/installsfcfssha611 -start node03 node04
   ```
4 When second half of the nodes come up, all the GAB ports a, b, d, h, u, v, w and f are ONLINE. Also all the CFS mounts service groups come online automatically.

5 Manually mount the VxFS and CFS file systems that are not managed by VCS in the second half of the cluster.

6 Find out which node is the CVM master. Enter the following:

```
# vxdctl -c mode
```

Performing phased upgrade of SF Oracle RAC to version 6.1.1

Table 4-2 illustrates the phased upgrade process. Each column describes the steps to be performed on the corresponding subcluster and the status of the subcluster when operations are performed on the other subcluster.

<table>
<thead>
<tr>
<th>First half of the cluster</th>
<th>Second half of the cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>SF Oracle RAC cluster before the upgrade:</td>
<td></td>
</tr>
</tbody>
</table>

**First half of the cluster**

- sys1
- sys2

**Second half of the cluster**

- sys3
- sys4

**STEP 1:** Perform the following pre-upgrade steps:

- Switch failover applications.
- Stop all parallel applications.

See “Step 1: Performing pre-upgrade tasks on the first half of the cluster” on page 122.

**STEP 2:** Upgrade SF Oracle RAC.

See “Step 2: Upgrading the first half of the cluster” on page 125.

The second half of the cluster is up and running.

- sys3
- sys4
Table 4-2  Summary of phased upgrade (continued)

<table>
<thead>
<tr>
<th>First half of the cluster</th>
<th>Second half of the cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>The first half of the cluster is not running.</td>
<td><strong>STEP 3</strong>: Perform the following pre-upgrade steps:</td>
</tr>
<tr>
<td>sys1</td>
<td>Stop all parallel and failover applications.</td>
</tr>
<tr>
<td>sys2</td>
<td>Stop SF Oracle RAC.</td>
</tr>
<tr>
<td></td>
<td>See “Step 3: Performing pre-upgrade tasks on the second half of the cluster” on page 126.</td>
</tr>
<tr>
<td></td>
<td>The downtime starts now.</td>
</tr>
</tbody>
</table>

**STEP 4**: Perform the following post-upgrade steps:

- Start SF Oracle RAC.
- Start all applications.

See “Step 4: Performing post-upgrade tasks on the first half of the cluster” on page 128.

The downtime ends here.

The first half of the cluster is up and running.

<table>
<thead>
<tr>
<th>sys1</th>
<th>sys2</th>
</tr>
</thead>
</table>

**STEP 5**: Upgrade SF Oracle RAC.

See “Step 5: Upgrading the second half of the cluster” on page 130.

**STEP 6**: Perform the following post-upgrade steps:

- Start SF Oracle RAC.
- Start all applications.

See “Step 6: Performing post-upgrade tasks on the second half of the cluster” on page 130.

The phased upgrade is complete and both the first and the second half of the cluster are running.

<table>
<thead>
<tr>
<th>sys1</th>
<th>sys2</th>
<th>sys3</th>
<th>sys4</th>
</tr>
</thead>
</table>

**Step 1: Performing pre-upgrade tasks on the first half of the cluster**

Perform the following pre-upgrade steps on the first half of the cluster.

- Stop all parallel and failover applications.
- Stop SF Oracle RAC.

See “Step 3: Performing pre-upgrade tasks on the second half of the cluster” on page 126.

The downtime starts now.

The first half of the cluster is not running.
To perform the pre-upgrade tasks on the first half of the cluster

1. **Back up the following configuration files:** main.cf, types.cf, CVMTypes.cf, CFSTypes.cf, OracleTypes.cf, OracleASMTypes.cf, PrivNIC.cf, MultiPrivNIC.cf, /etc/llttab, /etc/llthosts, /etc/gabtab, /etc/vxfentab, /etc/vxfendg, /etc/vxfenmode

   For example:

   ```
   # cp /etc/VRTSvcs/conf/config/main.cf \
   /etc/VRTSvcs/conf/config/main.cf.save
   # cp /etc/VRTSvcs/conf/config/types.cf \
   /etc/VRTSvcs/conf/config/types.cf.save
   # cp /etc/VRTSvcs/conf/config/OracleTypes.cf \
   /etc/VRTSvcs/conf/config/OracleTypes.cf.save
   # cp /etc/VRTSvcs/conf/config/PrivNIC.cf \
   /etc/VRTSvcs/conf/config/PrivNIC.cf.save
   # cp /etc/VRTSvcs/conf/config/MultiPrivNIC.cf \
   /etc/VRTSvcs/conf/config/MultiPrivNIC.cf.save
   ```

2. Installer verifies that recent backups of configuration files in VxVM private region have been saved in /etc/vx/cbr/bk.

   If not, a warning message will be displayed after installmr upgrade prechecks.

   **Warning:** Backup /etc/vx/cbr/bk directory.

3. If you plan to continue using StorageCheckpoint or storage tiering policies you created with a 5.0x or earlier version of Storage Foundation for Oracle RAC, complete the following preparatory step before migrating the SFDB repository database to 6.1.1.

   See "Pre-upgrade tasks for migrating the SFDB repository database" on page 35.

4. Stop all applications that are not configured under VCS but dependent on Oracle RAC or resources controlled by VCS. Use native application commands to stop the application.

5. Stop the applications configured under VCS. Stop the Oracle RAC database:
   - If the Oracle RAC instance is managed by VCS:
     ```
     # hagrp -offline oracle_group -sys node01
     # hagrp -offline oracle_group -sys node02
     ```
If the Oracle RAC instance is not managed by VCS, log in as the Oracle user on one of the nodes in the first half of the cluster and shut down the instances:

For Oracle RAC 12c:

```
$ srvctl stop instance -db db_name \\ 
   -node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl stop instance -d db_name \\ 
   -n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl stop instance -d db_name \\ 
   -i instance_name
```

If the Oracle database is managed by VCS, set the AutoStart value to 0 to prevent the database service group from starting automatically when VCS starts:

```
# haconf -makerw
# hagrp -modify oracle_group AutoStart 0
# haconf -dump -makero
```

If the Oracle database is not managed by VCS, change the management policy for the database to manual:

For Oracle RAC 12c:

```
$ srvctl modify database -db db_name -policy MANUAL
```

For Oracle RAC 11g:

```
$ srvctl modify database -d db_name -y MANUAL
```

Unmount the CFS file systems that are not managed by VCS.

Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:

```
# mount | grep vxfs | grep cluster

# fuser -cu /mount_point
```
■ Unmount the non-system CFS file system:
  
  ```
  # umount /mount_point
  ```

8 If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the `installmr` script:

  ```
  # sfcache offline cache_area
  ```

9 Stop the parallel service groups and switch over failover service groups on each of the nodes in the first half of the cluster:

  ```
  # hastop -local -evacuate
  ```

10 Unmount the VxFS file systems that are not managed by VCS.

■ Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:

  ```
  # mount | grep vxfs
  # fuser -cu /mount_point
  ```

■ Unmount the non-system VxFS file system:

  ```
  # umount /mount_point
  ```

11 Verify that no VxVM volumes (other than VxVM boot volumes) remain open. Stop any open volumes that are not managed by VCS.

12 If you plan to upgrade the operating system, stop all ports.

  ```
  # /opt/VRTS/install/installsfrac -stop node01 node02
  ```

**Step 2: Upgrading the first half of the cluster**

Perform the following steps to upgrade the first half of the cluster.
To upgrade the first half of the cluster

1. If you plan to upgrade the operating system, rename the `/etc/llttab` file to prevent LLT from starting automatically when the node starts:

   ```
   # mv /etc/llttab /etc/llttab.save
   ```

2. Upgrade the operating system, if required.

   For instructions, see the operating system documentation.

3. If you upgraded the operating system, restart the nodes:

   ```
   # shutdown -r now
   ```

4. Rename the `/etc/llttab` file to its original name:

   ```
   # mv /etc/llttab.save /etc/llttab
   ```

5. Make sure that you can run secure shell or remote shell from the node where you launched the installer to the nodes in the second subcluster without requests for a password.

6. Upgrade SF Oracle RAC. On the first half of the cluster, upgrade SFRAC by using the `installmr` script. For example use the `installmr` script as shown below:

   ```
   # ./installmr node01 node02
   ```

   **Note:** After you complete the upgrade of the first half of the cluster, no GAB ports will be shown in the output when you run the `gabconfig -a` command.

---

**Step 3: Performing pre-upgrade tasks on the second half of the cluster**

Perform the following pre-upgrade steps on the second half of the cluster.
To perform the pre-upgrade tasks on the second half of the cluster

1. Stop all applications that are not configured under VCS but dependent on Oracle RAC or resources controlled by VCS. Use native application commands to stop the application.

   Note: The downtime starts now.

2. If you plan to continue using Storage Checkpoint or storage tiering policies you created with a 5.0x or earlier version of Storage Foundation for Oracle RAC, complete the following preparatory step before migrating the SFDB repository database to 6.1.1.

   See "Pre-upgrade tasks for migrating the SFDB repository database" on page 35.

3. Stop all applications that are configured under VCS. Stop the Oracle RAC database:

   - If the Oracle RAC instance is managed by VCS:
     
     ```
     # hagrp -offline oracle_group -sys node03
     # hagrp -offline oracle_group -sys node04
     ```

   - If the Oracle RAC instance is not managed by VCS, log in as the Oracle user on one of the nodes in the second half of the cluster and shut down the instances:
     For Oracle RAC 12c:
     
     ```
     # srvctl stop instance -db db_name \ -node node_name
     ```

     For Oracle RAC 11.2.0.2 and later versions:
     
     ```
     $ srvctl stop instance -d db_name \ -n node_name
     ```

     For Oracle RAC 11.2.0.1 and earlier versions:
     
     ```
     $ srvctl stop instance -d db_name \ -i instance_name
     ```

4. Unmount the CFS file systems that are not managed by VCS.
■ Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:

# mount | grep vxfs | grep cluster
# fuser -cu /mount_point

■ Unmount the non-system VxFS file system:

# umount /mount_point

5 If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the installmr script:

# sfcache offline cache_area

6 Stop VCS on each of the nodes in the second half of the cluster:

# hastop -local

7 Unmount the VxFS file systems that are not managed by VCS.

■ Make sure that no processes are running which make use of mounted shared file system. To verify that no processes use the VxFS or CFS mount point:

# mount | grep vxfs
# fuser -cu /mount_point

■ Unmount the non-system VxFS file system:

# umount /mount_point

8 Verify that no VxVM volumes (other than VxVM boot volumes) remain open. Stop any open volumes that are not managed by VCS.

9 Stop all ports.

# /opt/VRTS/install/installslfrac -stop node03 node04

Step 4: Performing post-upgrade tasks on the first half of the cluster

Perform the following post-upgrade steps on the first half of the cluster.
To perform the post-upgrade tasks on the first half of the cluster

1. On any one node on the first half of the cluster, force GAB to form a cluster.
   
   ```
   # /etc/init.d/llt start
   # /etc/init.d/gab start
   # gabconfig -x
   ```

2. On the first half of the cluster, start SF Oracle RAC:
   
   ```
   # cd /opt/VRTS/install
   # ./installsfrac611 -start node01 node02
   ```

3. On the first half of the cluster, manually mount the VxFS or CFS file systems that are not managed by VCS.

4. Relink the SF Oracle RAC libraries with Oracle.

5. Bring the Oracle database service group online.
   
   If the Oracle database is managed by VCS:
   
   ```
   # hagrp -online oracle_group -sys node_name
   ```
   
   If the Oracle database is not managed by VCS:
   
   For Oracle RAC 12c:
   
   ```
   $ srvctl start instance -db db_name \
   -node node_name
   ```
   
   For Oracle RAC 11.2.0.2 and later versions:
   
   ```
   $ srvctl start instance -d db_name \
   -n node_name
   ```
   
   For Oracle RAC 11.2.0.1 and earlier versions:
   
   ```
   $ srvctl start instance -d db_name \
   -i instance_name
   ```

   **Note:** The downtime ends here.

6. On the first half of the cluster, start all applications that are not managed by VCS. Use native application commands to start the applications.
Step 5: Upgrading the second half of the cluster

Perform the following steps to upgrade the second half of the cluster.

To upgrade the second half of the cluster

1. If you plan to upgrade the operating system, rename the /etc/llttab file to prevent LLT from starting automatically when the node starts:
   
   ```
   # mv /etc/llttab /etc/llttab.save
   ```

2. Upgrade the operating system, if required.
   
   For instructions, see the operating system documentation.

3. If you upgraded the operating system, restart the nodes:
   
   ```
   # shutdown -r now
   ```

4. Rename the /etc/llttab file to its original name:
   
   ```
   # mv /etc/llttab.save /etc/llttab
   ```

5. Make sure that you can run secure shell or remote shell from the node where you launched the installer to the nodes in the first subcluster without requests for a password.

6. On the second half of the cluster, upgrade SF Oracle RAC. Navigate to the product directory on the installation media.
   
   Upgrade SFRAC by using the `installmr` script. For example use the `installmr` script as shown below:
   
   ```
   # ./installmr node03 node04
   ```

Step 6: Performing post-upgrade tasks on the second half of the cluster

Perform the following post-upgrade steps on the second half of the cluster.

To perform the post-upgrade tasks on the second half of the cluster

1. Manually mount the VxFS and CFS file systems that are not managed by VCS.

2. On the second half of the cluster, start SF Oracle RAC:
   
   ```
   # cd /opt/VRTS/install
   
   # ./installssfrac611 -start node03 node04
   ```
3 Relink the SF Oracle RAC libraries with Oracle.

4 Upgrade VxVM disk group version.

All Veritas Volume Manager disk groups have an associated version number. Each VxVM release supports a specific set of disk group versions and can import and perform tasks on disk groups with those versions. Some new features and tasks work only on disk groups with the current disk group version. Before you can perform the tasks, you need to upgrade existing disk group version to 180.

Check the existing disk group version:

    # vxdg list dg_name | grep -i version

If the disk group version is not 180, run the following command on the master node to upgrade the version:

    # vxdg -T 180 upgrade dg_name
5 Upgrade disk layout version.

In this release, you can create and mount only file systems with disk layout Version 7, 8, and 9. You can only local mount disk layout Version 6 only to upgrade to a later disk layout version.

Disk layout Version 6 has been deprecated and you cannot cluster mount an existing file system that has disk layout Version 6. To upgrade a cluster file system with disk layout Version 6, you must local mount the file system and then upgrade the file system using the `vxupgrade` utility to a later version.

See the `vxupgrade(1M)` manual page.

Support for disk layout Version 4 and 5 has been removed. You must upgrade any existing file systems with disk layout Version 4 or 5 to disk layout Version 7 or later using the `vxfsconvert` command.

See the `vxfsconvert(1M)` manual page.

---

**Note:** Symantec recommends that you upgrade existing file systems to the highest supported disk layout version prior to upgrading to this release.

You can check which disk layout version your file system has by using the following command:

```bash
# fstyp -v /dev/vx/dsk/dg1/vol1 | grep -i version
```

For more information about disk layout versions, see the Symantec™ Storage Foundation Administrator's Guide.
6 Bring the Oracle database service group online.

If the Oracle database is managed by VCS:

```shell
# hagrp -online oracle_group -sys node03
# hagrp -online oracle_group -sys node04
```

If the Oracle database is not managed by VCS:

For Oracle RAC 12c:

```shell
$ srvctl start instance -db db_name \ node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```shell
$ srvctl start instance -d db_name \ -n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```shell
$ srvctl start instance -d db_name \ -i instance_name
```

7 If the Oracle database is managed by VCS, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

```shell
# haconf -makerw
# hagrp -modify oracle_group AutoStart 1
# haconf -dump -makero
```

If the Oracle database is not managed by VCS, change the management policy for the database to automatic:

For Oracle RAC 12c:

```shell
$ srvctl modify database -db db_name -policy AUTOMATIC
```

For Oracle RAC 11g:

```shell
$ srvctl modify database -d db_name -y AUTOMATIC
```

8 Start all applications that are not managed by VCS. Use native application commands to start the applications.
9  Set or change the product license level, if required.

10  Migrate the SFDB repository database.
    
    As root, dump out the old Sybase Adaptive Server Anywhere (Sybase ASA) repository. If you are using SFHA or SF Oracle RAC, you only need to do this on one node.
    
    # /opt/VRTSdbed/migrate/sfua_rept_migrate

Upgrading to 6.1.1 on a system that has encapsulated boot disk

You can use this procedure to upgrade to 6.1.1 on a system that has encapsulated boot disk.

---

**Note:** Upgrading with encapsulated boot disk from 6.1 to 6.1.1 requires reboot.

---

To upgrade to 6.1.1 on a system that has encapsulated boot disk

1  If you have VxVM or VxFScache on your system, offline the cache.

    # sfcache offline cache_area

2  Manually unmount filesystems and stop open volumes.

3  Upgrade to 6.1.1 using `installmr` command.

4  After upgrading, reboot the system to have the new VM drivers take effect.

5  If the mirror of boot disk is split during upgrading, re-join the mirrors manually when systems reboot after upgrading to 6.1.1.

---

Performing a rolling upgrade using the installer

You can use rolling upgrades to upgrade one product from a release to the next with minimal application downtime.

- About rolling upgrades
- Prerequisites for a rolling upgrade
- Performing a rolling upgrade on kernel packages for VCS, SFHA and SFCFSHA: phase 1
Performing a rolling upgrade on non-kernel packages for VCS, SFHA and SFCFSHA: phase 2

Performing a rolling upgrade on kernel packages for SF Oracle RAC: phase 1

Performing a rolling upgrade on non-kernel packages for SF Oracle RAC: phase 2

About rolling upgrades

You can use rolling upgrades to upgrade one product from a release to the next. Rolling upgrades require less downtime.

Rolling upgrades take two discrete phases. In the first, you upgrade the kernel packages with exception of VCS packages and agent packages. In the second, you upgrade the non-kernel packages, which are VCS packages and agents packages.

You can perform a rolling upgrade for the following products:

- Symantec Cluster Server
- Storage Foundation and High Availability
- Storage Foundation Cluster File System High Availability
- Storage Foundation for Oracle RAC
- Symantec VirtualStore
- Storage Foundation for Sybase CE

Prerequisites for a rolling upgrade

Meet the following prerequisites before performing a rolling upgrade:

- Make sure that the product you want to upgrade supports rolling upgrades.
- Make a plan on splitting up your clusters into sub-clusters for the purpose of upgrade. A sub-cluster can include one or more nodes. This division helps to keep service groups running during the upgrade.
- Make sure you are logged in as superuser.
- VCS must be running before performing the rolling upgrade.
- Make sure you have downloaded the latest software required for the upgrade.

Limitation: During VCS and agents upgrade, you must bring down the application High Availability (HA) for several minutes. This does not affect the application running on the cluster. You can restore the application's high availability after VCS and the agent packages are upgraded.
Performing a rolling upgrade using the installer

You can use rolling upgrades to upgrade one product from a release to the next with minimal application downtime.

Performing a rolling upgrade on kernel packages for VCS, SFHA and SFCFSHA: phase 1

Note that in the following instructions a sub-cluster can represent one or more nodes in a full cluster, but is represented by nodeA as subcluster1 and nodeB as subcluster2.

To perform the rolling upgrade on kernel packages: phase 1

1. If you have VxVM or VxFS cache on your system, offline the cache before upgrading with the installmr script:

   ```bash
   # sfcache offline cache_area
   ```

2. On the first sub-cluster, start the installer for the rolling upgrade with the -rollingupgrade_phase1 option.

   ```bash
   # ./installmr -rollingupgrade_phase1 nodeA
   ```

   You can also use the web-based installer to perform the upgrade. If you are using the web-based installer, start the web-based installer with the ./webinstaller start command, select Rolling Upgrade from the task list, make sure the Phase-1: Upgrade Kernel packages radio button is checked, and then click Next.

3. Note that if the boot-disk is encapsulated, then you do not need to perform an unencapsulation for upgrades.

4. The installer checks system communications, package versions, product versions, and completes prechecks. It then upgrades applicable kernel patches.

   If you are using the web-based installer, input one node of the cluster. The web-based installer detects the whole cluster, and then recommend some nodes (NodeA) as the subcluster to run the rolling upgrade phase 1. The web-based installer checks system communications, package versions, product versions, and completes prechecks. It then upgrades applicable kernel packages.

5. The installer loads new kernel modules and starts all the relevant processes and brings all the service groups online.

6. If the boot disk is encapsulated, reboot the first sub-cluster's system. Otherwise go to step 7.
7 After rolling upgrade phase 1 is completed on node A, the following message displays:

It is recommended to perform rolling upgrade phase 1 on the systems node B in the next step.

Would you like to perform rolling upgrade phase 1 on the systems? [y,n,q] (y)

If you choose y, it continues to run rolling upgrade phase 1 by itself on node B.

If you choose n or q, you need to complete step 2 to step 5 on node B.

8 After rolling upgrade phase 1 of the cluster, the following message displays:

Would you like to perform rolling upgrade phase 2 on the cluster? [y,n,q] (y)

- If you choose y, it continues to run rolling upgrade phase 2 of the cluster by itself. You don't need to run phase 2:
  After phase 2 upgrade, verify the cluster's status:
  
  # hastatus -sum

- If you choose n or q, you need to use the following steps to finish rolling upgrade phase 2 of the cluster:

Performing a rolling upgrade on non-kernel packages for VCS, SFHA and SFCFSHA : phase 2

In this phase installer installs all non-kernel packages on all the nodes in cluster and restarts VCS cluster.
To perform the rolling upgrade on non-kernel packages: phase 2

1. Start the installer for the rolling upgrade with the `-rollingupgrade_phase2` option. Specify all the nodes in the cluster:

```
# ./installmr -rollingupgrade_phase2 nodeA nodeB nodeC nodeD
```

You can also use the web-based installer to perform the upgrade. If you are using the web-based installer, select **Rolling Upgrade** from the task list, make sure the **Phase-2: Upgrade non Kernel packages** radio button is checked, and then click **Next**.

2. The installer checks system communications, patch versions, product versions, and completes prechecks. It upgrades non-kernel patches. It also verifies completion of phase 1.

   If you are using the web-based installer, input one node of the cluster, the web-based installer detects the whole cluster to run the rolling upgrade phase 2. The web-based installer checks system communications, package versions, product versions, and completes prechecks. It verifies completion of phase 1.

3. Installer will start HA daemon (had) on all nodes, HA will be available once HA daemon is up.

4. Verify the cluster’s status:

```
# hastatus -sum
```

5. If you want to upgrade CP server systems that use VCS or SFHA to 6.1, make sure that you upgraded all application clusters to version 6.1. Then, upgrade VCS or SFHA on the CP server systems.

For instructions to upgrade VCS or SFHA on the CP server systems, see the VCS or SFHA installation guide.

**Performing a rolling upgrade on kernel packages for SF Oracle RAC: phase 1**

Note that in the following instructions that a subcluster can represent one or more nodes in a full cluster, but is represented by nodeA, nodeB as subcluster1 and nodeC, nodeD as subcluster2.
To perform the rolling upgrade on kernel: phase 1

1. Log in as superuser to one of the nodes in the cluster.

2. Back up the following configuration files on your system: `main.cf`, `types.cf`, `CVMTypes.cf`, `CFSTypes.cf`, `OracleTypes.cf`, `OracleASMTypes.cf`, `PrivNIC.cf`, `MultiPrivNIC.cf`, `/etc/llttab`, `/etc/llthosts`, `/etc/gabtab`, `/etc/vxfentab`, `/etc/vxfendg`, `/etc/vxfenmode`.

   For example:

   ```
   # cp /etc/VRTSvcs/conf/config/main.cf /etc/VRTSvcs/conf/config/main.cf.save
   # cp /etc/VRTSvcs/conf/config/types.cf /etc/VRTSvcs/conf/config/types.cf.save
   # cp /etc/VRTSvcs/conf/config/OracleTypes.cf /etc/VRTSvcs/conf/config/OracleTypes.cf.save
   # cp /etc/VRTSvcs/conf/config/PrivNIC.cf /var/tmp/PrivNIC.cf.save
   # cp /etc/VRTSvcs/conf/config/MultiPrivNIC.cf /var/tmp/MultiPrivNIC.cf.save
   ```

3. If the Oracle database is managed by VCS, set the AutoStart value to 0 to prevent the database service group from starting automatically when VCS starts. Failing to perform this step results in the database attempting to come online after the upgrade; the attempt fails due to the presence of old libraries on the system.

   ```
   # haconf -makerw
   # hagrp -modify oracle_group AutoStart 0
   # haconf -dump -makero
   ```

   If the Oracle database is not managed by VCS, change the management policy for the database to manual:

   For Oracle RAC 11g:

   `$ srvctl modify database -d db_name -y MANUAL`

   For Oracle RAC 12c:

   `$ srvctl modify database -db db_name -policy MANUAL`
4 Stop the applications that use VxFS or VxVM disk groups on each node, whether local or CFS.
   If the applications are under VCS control:
   
   ```
   # hagrp -offline grp_name -sys node_name
   ```
   
   If the applications are not under VCS control:
   
   Use native application commands to stop the application.

5 Stop the Oracle RAC resources on each node.
   
   ■ If the database instances are managed by VCS, take the corresponding VCS service groups offline. As superuser, enter:
   
   ```
   # hagrp -offline oracle_group -sys nodeA
   # hagrp -offline oracle_group -sys nodeB
   ```
   
   ■ If the database instances are not managed by VCS, then run the following on one node:
   
   For Oracle RAC 12 c:
   
   ```
   $ srvctl stop instance -db db_name -node node_name
   ```
   
   For Oracle RAC 11.2.0.2 and later versions:
   
   ```
   $ srvctl stop instance -d db_name \
   -n node_name
   ```
   
   For Oracle RAC 11.2.0.1 and earlier versions:
   
   ```
   $ srvctl stop instance -d db_name \
   -i instance_name
   ```

6 Switch over all failover service groups to the other nodes in the cluster:

   ```
   # hagrp -switch grp_name -to node_name
   ```

7 Take all the VCS service groups offline:

   ```
   # hagrp -offline grp_name -sys node_name
   ```
8 Unmount all the VxFS file system which is not under VCS control.

# mount |grep vxfs
# fuser -m /mount_point
# umount /mount_point

Make sure that no processes are running which make use of mounted shared file system or shared volumes.

# fuser -cu /mount_point

Note: Installer will automatically stop all the applications, database instances, filesystems and volumes which are under VCS control on nodes, while using the rollingupgrade_phase1 option.

9 On the sub-cluster, start the installer for the rolling upgrade with the -rollingupgrade_phase1 option.

# ./installmr -rollingupgrade_phase1 nodeA nodeB

You can also use the web-based installer to perform the upgrade. If you are using the web-based installer, start the web-based installer with the ./webinstaller start command, select Rolling Upgrade from the task list, make sure the Phase-1: Upgrade Kernel packages radio button is checked, and then click Next.

10 Note that if the boot-disk is encapsulated, you do not need to perform an unencapsulation for upgrades.

11 The installer checks system communications, package versions, product versions, and completes prechecks. It then upgrades applicable kernel patches. If you are using the web-based installer, input one node of the cluster. The web-based installer detects the whole cluster, and then recommend some nodes (NodeA) as the subcluster to run the rolling upgrade phase 1. The web-based installer checks system communications, package versions, product versions, and completes prechecks. It then upgrades applicable kernel.

12 Relink the SF Oracle RAC libraries with Oracle:

Choose the option Relink Oracle Database Binary from the program menu.
13 When prompted, choose the option "Continue Rolling Upgrade" from the menu:

1) Relink Oracle Database Binary
2) Continue Rolling Upgrade

Choose option: [1-2,q] (1) 2

14 If the boot disk is encapsulated, the installer strongly recommends a reboot of the nodes. Reboot the nodes as prompted by the installer.

15 For minimal down time, bring the oracle groups and database up manually on sub-cluster on which phase 1 is completed:

- If the database instances are managed by VCS, take the corresponding VCS service groups online. As superuser, enter:

  # hagrp -online oracle_group -sys nodeA
  # hagrp -online oracle_group -sys nodeB

- If the database instances are not managed by VCS, then run the following on one node:
  For Oracle RAC 12c:

  # srvctl start instance -db db_name -node node_name

  For Oracle RAC 11.2.0.2 and later versions:

  # $ srvctl start instance -d db_name -n node_name

  For Oracle RAC 11.2.0.1 and earlier versions:

  # $ srvctl start instance -d db_name -i instance_name

16 Manually mount the VxFS and CFS file systems that are not managed by VCS.

17 Bring the Oracle database service group online.

- If VCS manages the Oracle database:

  # hagrp -online oracle_group -sys node_name

- If VCS does not manage the Oracle database:
For Oracle RAC 12c:

```
$ srvctl start instance -db db_name \
   -node node_name
```

For Oracle RAC 11.2.0.2 and later versions:

```
$ srvctl start instance -d db_name \
   -n node_name
```

For Oracle RAC 11.2.0.1 and earlier versions:

```
$ srvctl start instance -d db_name \
   -i instance_name
```

18 Start all applications that are not managed by VCS. Use native application commands to start the applications.

19 After rolling upgrade phase 1 is completed on nodeA and nodeB, the following message displays:

```
It is recommended to perform rolling upgrade phase 1 on the systems nodeC and nodeD in the next step.
```

Would you like to perform rolling upgrade phase 1 on the systems? [y,n,q] (y)

- If you choose y, first complete step 4 to step 8 on the remaining subcluster. Then it continues to run rolling upgrade phase 1 on nodeC and nodeD by itself.
- If you choose n or q, go to step 15.

20 After rolling upgrade phase 1 of the cluster, the following message displays:

```
Would you like to perform rolling upgrade phase 2 on the cluster? [y,n,q] (y)
```

- If you choose y, it continues to run rolling upgrade phase 2 of the cluster by itself. You don’t need to run phase 2: See “Performing a rolling upgrade on non-kernel packages for SF Oracle RAC: phase 2” on page 144. After rolling upgrade phase 2, complete step 19 to step 22 (except step 21) verify the cluster’s status:
  
  ```
  # hastatus --sum
  ```

- If you choose n or q, you need to complete step 19 to step 22 and run rolling upgrade phase 2: See “Performing a rolling upgrade on non-kernel packages for SF Oracle RAC: phase 2” on page 144.
Before you proceed to phase 2, complete step 4 to 18 on the remaining subcluster.

Perform one of the following steps:

- If VCS manages the Oracle database, reset the AutoStart value to 1 to enable VCS to bring the database service group online automatically when VCS starts:

  ```
  # haconf -makerw
  # hagrp -modify oracle_group AutoStart 1
  # haconf -dump -makero
  ```

- If the VCS does not manage the Oracle database, change the management policy for the database to automatic:
  For Oracle RAC 12c:

  ```
  $ srvctl modify database -db db_name -policy AUTOMATIC
  ```

  For Oracle RAC 11g:

  ```
  $ srvctl modify database -d db_name -y AUTOMATIC
  ```

Performing a rolling upgrade on non-kernel packages for SF Oracle RAC: phase 2

In this phase, the installer installs all non-kernel RPMs on all the nodes in cluster and restarts VCS cluster.

To perform the rolling upgrade on non-kernel packages: phase 2

1. Start the installer for the rolling upgrade with the `-rollingupgrade_phase2` option. Specify all the nodes in the cluster:

   ```
   ./installmr -rollingupgrade_phase2 nodeA nodeB nodeC nodeD
   ```

   You can also use the web-based installer to perform the upgrade. If you are using the web-based installer, select Rolling Upgrade from the task list, make sure the Phase-2: Upgrade non Kernel packages radio button is checked, and then click Next.

2. The installer checks system communications, package versions, product versions, and completes prechecks. It verifies completion of phase 1.

   If you are using the web-based installer, input one node of the cluster, the web-based installer detects the whole cluster to run the rolling upgrade phase 2. The web-based installer checks system communications, package versions, product versions, and completes prechecks. It verifies completion of phase 1.
3 Installer will start HA daemon (had) on all nodes, HA will be available once HA daemon is up.

4 Verify the cluster's status:

   # hastatus -sum

Upgrading the operating system

This section describes how to upgrade the operating system on a Symantec Storage Foundation and High Availability Solutions (SFHA) node where you plan to upgrade to 6.1.1 for Red Hat Enterprise Linux (RHEL) 5, RHEL 6, SUSE Linux Enterprise (SLES) 10, SLES 11, Oracle Linux (OL) 5, and OL 6.

Preparing for OS upgrades

1 Rename the /etc/llttab file to prevent LLT from starting automatically when the node starts:

   # mv /etc/llttab /etc/llttab.save

2 Upgrade the operating system on all nodes in the cluster.

   For instructions, see the operating system documentation.

   Note: If required, restart the nodes with the `shutdown -r now` command.

3 After the system restarts, restore the /etc/llttab file to its original name:

   # mv /etc/llttab.save /etc/llttab

To upgrade the operating system to a later version

1 Stop Storage Foundation.

2 Upgrade to the latest operating system.

3 Upgrade to 6.1.1.

4 Start Storage Foundation.

Upgrading SFHA with the Veritas Web-based installer

This section describes upgrading SFHA with the Veritas Web-based installer. The installer detects and upgrades the product that is currently installed on the specified
system or systems. If you want to upgrade to a different product, you may need to perform additional steps.

To perform a full upgrade for SFHA

1. Perform the required steps to save any data that you wish to preserve. For example, take back-ups of configuration files.
2. Start the Web-based installer.
3. On the Select a task and a product page, select Install 6.1.1 from the Task drop-down list, and click Next.
4. Stop all applications accessing the file system. Unmount all mounted filesystems before installation.
5. Indicate the systems on which to upgrade. Enter one or more system names, separated by spaces. Click Next.

   The installer detects the product that is installed on the specified system.
6. The installer stops the processes. Choose to restore and reuse the previous configuration on all systems. Click Next to start the processes.
7. Click Next to complete the upgrade.

   After the upgrade completes, the installer displays the location of the log and summary files. If required, view the files to confirm the installation status.
8. Click Finish. The installer prompts you for another task.

To perform a rolling upgrade with Veritas Web-based installer, refer to 6.1 Installation Guides for your products.

Verifying software versions

To list the Symantec RPMs installed on your system, enter the following command:

```
# rpm -qa | grep VRTS
```

The output version for 6.1.1 is 6.1.1.000, and the VRTSperl version is 5.14.2.20.
Removing Symantec Storage Foundation and High Availability Solutions

This chapter includes the following topics:

- About removing Symantec Storage Foundation and High Availability Solutions 6.1.1
- Uninstalling Symantec Storage Foundation Cluster File System High Availability 6.1.1
- Uninstalling Symantec Storage Foundation for Oracle RAC

About removing Symantec Storage Foundation and High Availability Solutions 6.1.1

Symantec recommends that you follow the steps in the following sections to remove all the installed Symantec software, and then perform a complete reinstallation of the previous release.

For extensive uninstallation and reinstallation procedures, refer to the appropriate product’s Installation Guide.
Uninstalling Symantec Storage Foundation Cluster File System High Availability 6.1.1

This section provides procedures for uninstalling Symantec Storage Foundation Cluster File System High Availability (SFCFSHA). You must complete the preparatory tasks before you uninstall SFCFS.

Preparing to uninstall Symantec Storage Foundation Cluster File System High Availability

The following procedure prepares your system for uninstalling Symantec Storage Foundation Cluster File System High Availability (SFCFSHA).

To prepare to uninstall Symantec Storage Foundation Cluster File System High Availability

1. Log in as the root user on any node in the cluster.
2. Verify that the following directories are set in your PATH environment variable:

   /optVRTS/bin
   /optVRTSvcs/bin

3. Back up the following configuration files:

   # mv /etc/llttab /etc/llttab.`date +%m-%d-%y%H%M%S`
   # mv /etc/llthosts /etc/llthosts.`date +%m-%d-%y%H%M%S`
   # mv /etc/gabtab /etc/gabtab.`date +%m-%d-%y%H%M%S`
   # mv /etc/vxfenmode /etc/vxfenmode.`date +%m-%d-%y%H%M%S`

4. Determine if each node’s root disk is under VxVM control and proceed as follows.
   - Check if each node’s root disk is under VxVM control:

     # df -v /

     The root disk is under VxVM control if /dev/vx/dsk/rootvol is listed as being mounted as the root (/) file system. If so, unmirror and unencapsulate the root disk as described in the following steps:
     - If the encapsulated root disk is mirrored, use the vxrootadm command to split the mirror.
       For example, the following command removes a root disk mirror from the current root disk group:
Enter the following command to convert all the encapsulated volumes in the root disk back to being accessible directly through disk partitions instead of through volume devices.

```
# /etc/vx/bin/vxunroot
```

Following the removal of encapsulation, the system is rebooted from the unencapsulated root disk.

5. If you have created any Volume Replicator (VVR) replicated volume groups (RVGs) on your system, perform the following steps:

- Stop all applications that are involved in replication. For example, if a data volume contains a file system, unmount it.
- Use the `vxrvg stop` command to stop each RVG individually:
  
  ```
  # vxrvg -g diskgroup stop rvg_name
  ```

- On the Primary node, use the `vxrlink status` command to verify that all RLINKs are up-to-date:

  ```
  # vxrlink -g diskgroup status rlink_name
  ```

6. Check if any VxFS file systems or Storage Checkpoints are mounted:

   ```
   # df -T | grep vxfs
   ```

7. Unmount all Storage Checkpoints and file systems:

   ```
   # umount /checkpoint1
   # umount /filesystem1
   ```

   If file system is mounted in a cluster, then use `cfsunmount` command.
Stop all VxVM volumes by entering the following command for each disk group:

```
# vxvol -g dg1 stopall
```

To verify that no volumes are open:

```
# vxprint -Aht -e v_open
```

Stop VCS:

```
# hastop -all
```

**Uninstalling Symantec Storage Foundation Cluster File System High Availability**

The following procedure uninstalls Symantec Storage Foundation Cluster File System High Availability (SFCFSHA).

**To uninstall Symantec Storage Foundation Cluster File System High Availability**

1. Log in as the root user on any node in the cluster.
2. Navigate to the directory that contains the uninstallation program:
   ```
   # cd /opt/VRTS/install
   ```
3. Run the uninstallation program while specifying each node in the cluster:
   ```
   # ./uninstallsfcfsha61 node01 node02
   ```
4. Confirm the uninstallation:
   ```
   Are you sure you want to uninstall SFCFSHA [y,n,q] (y)
   ```

   The installer stops the Symantec Storage Foundation Cluster File System High Availability processes and uninstalls the packages.

Uninstalling Symantec Storage Foundation for Oracle RAC

The following procedure uninstalls Symantec Storage Foundation for Oracle RAC (SFRAC).

**Note:** This procedure will remove the complete SFRAC stack from all nodes.

**To uninstall Symantec Storage Foundation for Oracle RAC**

1. On each node, take the Oracle resources in the VCS configuration file (`main.cf`) offline.
   
   ```bash
   # hagrp -offline oracle_group -sys node_name
   ```
   
   If the database is not managed by VCS, stop the Oracle database as follows:
   
   ```bash
   $ srvctl stop database -d db_name
   ```

2. If Oracle Clusterware is not under VCS Control, then enter the following command on each node of the cluster to stop Oracle Clusterware.
   - For 11gR2 and 12c:
     
     ```bash
     # /etc/init.d/ohasd stop
     ```

3. Stop the applications that use CVM or CFS that are not under VCS control
   - Using native application commands, stop the applications that use CVM or CFS on all nodes.
   - Verify that no processes use the CFS mount point:
     
     ```bash
     # fuser -c /mount_point
     ```

4. Unmount CFS file systems that are not under VCS control
   - Determine the file systems that need to be unmounted by checking the output of mount command.
     
     ```bash
     # mount -v | grep vxfs | grep cluster
     ```
   - Unmount each file system that is not controlled by VCS on each node:
     
     ```bash
     # umount /mount_point
     ```
5 If you have VxVM or VxFS cache on your system, offline the cache before uninstallation:

   # sfcache offline cache_area

6 Stop VCS to take the service groups on all nodes offline

   On any one node execute following command to stop VCS:

   # hastop -all

7 Stopping the applications that use VxVM or VxFS that are not under VCS control

   ■ Using native application commands, stop the applications that use VxVM or VxFS.

   ■ Verify that no processes use the VxFS mount point:

   # fuser -c /mount_point

8 Unmounting VxFS file systems that are not under VCS control.

   ■ Determine the file systems that need to be unmounted by checking the output of mount command.

   # mount -v | grep vxfs

   Unmount each file system that is not controlled by VCS on each node:

   # umount /mount_point

9 Remove SF for Oracle RAC.

   ■ On any one node, navigate to the directory that contains the uninstallsfarc program:

   # cd /opt/VRTS/install

   ■ Start the uninstallsfarc program:

   # ./uninstallsfarc61

10 After uninstalling the SF Oracle RAC, refer to the chapter of *Installing the products for the first time* in this document to reinstall the SF Oracle RAC 6.1.1 software.
About the installation script

This appendix includes the following topics:

- About the installation script

About the installation script

Symantec™ Storage Foundation and High Availability Solutions 6.1.1 provides an installation and upgrade script. To install or upgrade the patches that are included in this release, you can use the `installmr` script. The `installmr` script lets you install or upgrade all the patches that are associated with the packages installed.

For more information regarding installation,

Symantec has introduced a new Install Bundles feature to help you install or upgrade directly to maintenance level with one execution. You can use the `-base_path` option to install or upgrade base and maintenance bundles. There are a few prerequisites for using Install Bundles feature for installation and upgrade of 6.1.1 mentioned below:

The `installmr` script options

The following table lists the command line options for the `installmr` and upgrade script:

<table>
<thead>
<tr>
<th>Table A-1</th>
<th>The command line options for the product <code>installmr</code> and upgrade script</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Line Option</td>
<td>Function</td>
</tr>
<tr>
<td><code>system1 system2...</code></td>
<td>Specifies the systems on which to run the installation options. A system name is required for all options. If not specified, the command prompts for a system name.</td>
</tr>
</tbody>
</table>
Table A-1  The command line options for the product installmr and upgrade script (continued)

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>-base_path</td>
<td>The -base_path option is used to define the path of a base level release to be integrated with a maintenance level release in order for the two releases to be simultaneously installed.</td>
</tr>
<tr>
<td>–precheck</td>
<td>Performs a preinstallation check to determine if systems meet all installation requirements. Symantec recommends doing a precheck before installing a product.</td>
</tr>
<tr>
<td>–postcheck</td>
<td>Checks any issues after installation or upgrading on the system.</td>
</tr>
<tr>
<td>–responsefile response_file</td>
<td>Automates installation and configuration by using system and configuration information stored in a specified file instead of prompting for information. The response_file must be a full path name. You must edit the response file to use it for subsequent installations. Variable field definitions are defined within the file.</td>
</tr>
<tr>
<td>–logpath log_path</td>
<td>Specifies a directory other than /opt/VRTS/install/logs as the location where installer log files, summary files, and response files are saved.</td>
</tr>
<tr>
<td>–tmppath tmp_path</td>
<td>Specifies a directory other than /var/tmp as the working directory for the installation scripts. This destination is where initial logging is performed and where RPMs are copied on remote systems before installation.</td>
</tr>
<tr>
<td>–timeout timeout_value</td>
<td>The –timeout option is used to specify the number of seconds that the script should wait for each command to complete before timing out. Setting the -timeout option overrides the default value of 1200 seconds. Setting the -timeout option to 0 will prevent the script from timing out. The -timeout option does not work with the -serial option</td>
</tr>
<tr>
<td>–keyfile ssh_key_file</td>
<td>Specifies a key file for secure shell (SSH) installs. This option passes –i ssh_key_file to every SSH invocation.</td>
</tr>
</tbody>
</table>
### Table A-1
The command line options for the product installmr and upgrade script (continued)

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>--hostfile <em>full_path_to_file</em></td>
<td>Specifies the location of a file that contains a list of hostnames on which to install.</td>
</tr>
<tr>
<td>-patchpath</td>
<td>The <code>-patchpath</code> option is used to define the complete path of a directory available to all install systems (usually NFS mounted) that contains all patches to be installed by installmr.</td>
</tr>
<tr>
<td>--kickstart <em>dir_path</em></td>
<td>Produces a kickstart configuration file for installing with Linux RHEL Kickstart. The file contains the list of Symantec RPMs in the correct order for installing, in a format that can be used for Kickstart installations. The <code>dir_path</code> indicates the path to the directory in which to create the file.</td>
</tr>
<tr>
<td>-yumgroupxml</td>
<td>The <code>-yumgroupxml</code> option is used to generate a yum group definition XML file. The <code>createrepo</code> command can use the file on Redhat Linux to create a yum group for automated installation of all rpms for a product. An available location to store the XML file should be specified as a complete path. The <code>-yumgroupxml</code> option is supported on Redhat Linux only.</td>
</tr>
<tr>
<td>-require</td>
<td>The <code>–require</code> option is used to specify a installer hot fix file.</td>
</tr>
<tr>
<td>–serial</td>
<td>Specifies that the installation script performs install, uninstall, start, and stop operations on each system in a serial fashion. If this option is not specified, these operations are performed simultaneously on all systems.</td>
</tr>
<tr>
<td>-rsh</td>
<td>Specifies this option when you want to use RSH and RCP for communication between systems instead of the default SSH and SCP.</td>
</tr>
<tr>
<td>--redirect</td>
<td>Displays progress details without showing the progress bar.</td>
</tr>
<tr>
<td>-pkgset</td>
<td>Discovers and displays the RPM group (minimum, recommended, all) and RPMs that are installed on the specified systems.</td>
</tr>
</tbody>
</table>
Table A-1: The command line options for the product installmr and upgrade script (continued)

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>–pkgtable</td>
<td>Displays product's RPMs in correct installation order by group.</td>
</tr>
<tr>
<td>–listpatches</td>
<td>The <code>–listpatches</code> option displays product patches in correct installation order.</td>
</tr>
<tr>
<td>–makeresponsefile</td>
<td>Use the <code>–makeresponsefile</code> option only to generate response files. No actual software installation occurs when you use this option.</td>
</tr>
<tr>
<td>–comcleanup</td>
<td>The <code>–comcleanup</code> option removes the secure shell or remote shell configuration added by installer on the systems. The option is only required when installation routines that performed auto-configuration of the shell are abruptly terminated.</td>
</tr>
<tr>
<td>–version</td>
<td>Checks and reports the installed products and their versions. Identifies the installed and missed RPMs and patches where applicable for the product. Provides a summary that includes the count of the installed and any missed RPMs and patches where applicable. Lists the installed patches, hotfixes, and available updates for the installed product if an Internet connection is available.</td>
</tr>
<tr>
<td>–nolic</td>
<td>Allows installation of product RPMs without entering a license key. Licensed features cannot be configured, started, or used when this option is specified.</td>
</tr>
<tr>
<td>-rolling_upgrade</td>
<td>Starts a rolling upgrade. Using this option, the installer detects the rolling upgrade status on cluster systems automatically without the need to specify rolling upgrade phase 1 or phase 2 explicitly.</td>
</tr>
<tr>
<td>–rollingupgrade_phase1</td>
<td>The <code>–rollingupgrade_phase1</code> option is used to perform rolling upgrade Phase-I. In the phase, the product kernel RPMs get upgraded to the latest version</td>
</tr>
</tbody>
</table>
Table A-1  The command line options for the product installmr and upgrade script (continued)

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>-rollingupgrade_phase2</td>
<td>The <code>-rollingupgrade_phase2</code> option is used to perform rolling upgrade Phase-II. In the phase, VCS and other agent RPMs upgrade to the latest version. Product kernel drivers are rolling-upgraded to the latest protocol version.</td>
</tr>
<tr>
<td>-disable_dmp_native_support</td>
<td>Disables Dynamic multi-pathing support for native the LVM volume groups/ZFS pools during an upgrade. Retaining Dynamic multi-pathing support for the native LVM volume groups/ZFS pools during an upgrade increases package upgrade time depending on the number of LUNs and native LVM volume groups/ZFS pools configured on the system. The <code>-disable_dmp_native_support</code> option is supported in upgrade scenario only.</td>
</tr>
<tr>
<td>-noipc</td>
<td>Disables the installer from making outbound networking calls to Symantec Operations Readiness Tool (SORT) in order to automatically obtain hot fixes and release information updates.</td>
</tr>
</tbody>
</table>